s-Familias profundas de Erdős

Mauricio Jafet Santos Camargo

Trabajo de Grado para Optar al Título de Matemático

Director:

Carlos Arturo Rodríguez Palma

Doctor en Matemáticas

Universidad Industrial de Santander

Facultad de ciencias

Escuela de Matemáticas

Matemáticas

Bucaramanga

2024

Dedicatoria

El presente trabajo esta dedicado a mi familia, en gratitud al apoyo incondicional brindado a lo largo de esta carrera profesional. Igualmente, dedico este logro a mi bella esposa, todo esto es gracias a ti, este trabajo y los futuros que construirás a mi lado.

Agradecimientos

A mi familia, por estar siempre presente, apoyando y contribuyendo en la culminación de cada meta.

A mi bella esposa, por su guía, su comprensión, su tiempo y sabiduría. Es por ti que todo esto es posible.

A todo aquel docente, que me ofreció su mano y una segunda oportunidad cuando más lo necesitaba.

A mis amigos y compañeros, por cada momento de risa y dispersión, de ayuda y trabajo, gracias a ustedes la culminación de este objetivo fue más amena.

A mi, por siempre perseverar y crecer con resiliencia y paciencia.

Tabla de contenido

Listas de tablas

Resumen

Título: s-Familias profundas de Erdős

Autor: Mauricio Jafet Santos Camargo

Palabras Clave: Conjuntos profundos de Erdős, enteros módulo n, cantidad de conjuntos, distancias.

Descripción: Dado un subconjunto C de $\mathbb{Z}_n$, se define ΔC como el multiconjunto de distancias entre elementos no iguales de C. Tomando como inspiración el problema del plano de Erdős, diremos que C es un conjunto profundo de Erdős en Z_n, si para cada $i \in \{1, 2, \ldots, k\}$, con $k = |C|$, existe una única distancia, entre elementos de C, tal que su multiplicidad (cantidad de veces que se repite cada distancia en ΔC) es i. El presente trabajo; en primer lugar, presenta un estudio y reformulación de los trabajos previamente realizados sobre la caracterización de todo conjunto profundo de Erdős en Z_n. Además, se establecen dos resultados que evidencian una forma de contar dichos conjuntos dependiendo de su tamaño y de Z_n. En segunda instancia, se establece el concepto de $s-$familia profunda de Erdős en Z_n y se estudian los resultados afines a este nuevo concepto, finalizando con una conjetura sobre la clasificación de las $2-$familias profundas de Erdős en Z_n.

Abstract

Title: s-Deep Families of Erdős

Author: Mauricio Jafet Santos Camargo

Palabras Clave: Deep sets of Erdős, integers modulo n, number of sets, distances.

Description: Given a subset C of $\mathbb{Z}_n$, ΔC is defined as the multiset of distances between unequal elements of C. Taking inspiration from the problem of the plane of Erdős, we will say that C is a Erdős-deep set in Z_n, if for each $i \in \{1, 2, \ldots, k\}$, with $k = |C|$, there is a single distance, between elements of C, such that its multiplicity (number of times each distance is repeated in ΔC) is i. The present work; first, it presents a study and reformulation of the work previously carried out on the characterization of any Erdős-deep set in Z_n. In addition, two results are established that show a way of counting these sets depending on their size and Z_n. In the second instance, the concept of $s-$ Erdős-deep families in Z_n is established and the results related to this new concept are studied, ending with a conjecture about the classification of the deep $2-$ Erdős-deep families in Z_n.

Introducción

Paul Erdős, en la década de los ochenta, se preguntó si era posible encontrar un conjunto de m puntos en el plano de tal manera que ninguno de cada tres de ellos estuviera sobre una recta, ni ninguno de cada cuatro de ellos estuviera en una circunferencia, y que para cada i, con $i = 1, \ldots, m-1$, existiera una distancia determinada por esos puntos que ocurriera exactamente i veces.

Tiempo después, Godfried Toussaint y otros investigadores se basaron en el problema postulado por Erdős para proponer una versión discreta del mismo. Este consiste en conseguir los subconjuntos de k puntos pertenecientes a un conjunto de n puntos espaciados uniformemente alrededor de una circunferencia y enumerados desde 0 hasta $n-1$, de manera que para cada j, con $j = 1, \ldots, k-1$, existe una distancia distinta de cero determinada por dos puntos sobre la circunferencia que ocurre exactamente j veces. Para este problema, los autores definieron la distancia entre dos puntos k_1 y k_2 como uno más la menor cantidad de puntos entre ellos sobre la circunferencia y la formularon como $d(k_1, k_2) = min\{|k_1 - k_2|, n - |k_1 - k_2|\}$. Los autores denominaron a estos conjuntos de puntos como ritmos profundos de Erdős.

Posteriormente, Gaede Tao recopila los estudios sobre ritmos profundos, incluyendo las investigaciones de Toussaint, y expande todos sus conceptos y resultados al contexto del espacio métrico $(\mathbb{Z}_n, \delta)$. Es así, que enuncia la primera reinterpretación de los ritmos profundos de Erdős como subconjuntos profundos de Erdős en $\mathbb{Z}_n$. No conforme con sus compendios monográficos introduce la noción de una familia profunda de Erdős conformada por s conjuntos profundos de Erdős (lo que se denominará en este trabajo como s-familias profundas de Erdős).

Inicialmente, este trabajo expone una caracterización de $\mathbb{Z}_n$ como subgrupo y como espacio métrico, junto con su relación con los grafos. Esto con el objetivo de fundamentar el estudio de las s-Familias profundas de Erdős, en especial, el caso $s = 1$ y el $s = 2$.

Seguidamente, se muestran las condiciones y las definiciones de los elementos que determinan si un conjunto es un conjunto profundo de Erdős en $\mathbb{Z}_n$. A partir de esto, se establecieron y se demostraron, de manera propia, una serie de lemas que son necesarios para establecer el teorema de caracterización de los conjuntos profundos de Erdős. Adicionalmente, se parte de dichos resultados para contar cuántos subconjuntos, de algún $\mathbb{Z}_n$, son conjuntos profundos de Erdős y de estos, contar cuantos tienen cierto

tamaño k. Por tanto, gran parte del trabajo está enfocado en el caso $s = 1$.

Con respecto al caso $s = 2$ se amplían las definiciones expuestas en el caso anterior y se presenta un teorema que permite caracterizar las 2-Familias profundas de Erdős, este teorema cuenta de dos partes, de las cuales solo se demuestra la primera, ya que para la demostración de la segunda se necesitan contenidos que no son mencionados en este trabajo. No obstante, se invita a ahondar sobre esta parte.

1. Objetivos

1.1. Objetivo general

Estudiar la caracterización de las s-Familias profundas de Erdős en los casos $s = 1$ y $s = 2$.

1.2. Objetivos específicos

- Recopilar conceptos y resultados acerca de los conjuntos profundos de Erdős y las s-familias profundas de Erdős (caso $s = 1$ y $s = 2$).
- Estudiar los elementos usados en las pruebas de los teoremas de caracterización de las s-familias profundas de Erdős para los casos $s = 1$ y $s = 2$.
- Procurar establecer problemas y resultados relacionados a las s-familias de Erdős.

2. Preliminares

Para dar comienzo al estudio de las s-familias de Erdős en $\mathbb{Z}_n$ es preciso definir el conjunto $\mathbb{Z}_n$, las operaciones entre sus elementos y como se miden distancias entre estos. Para ello, se considerará un conjunto y definiciones auxiliares que se enunciarán en las siguientes secciones de este capítulo y las cuales ayudarán a definir nuestro conjunto de interés y sus características.

2.1. Enteros módulo n

Definición 2.1 (Congruencia)**.** Sea $x, y \in \mathbb{Z}$ y $n \in \mathbb{N}$. Si $n \mid (x - y)$, se dice que x es **congruente** con y módulo n y se escribe

$$x \equiv y \pmod{n}. \tag{1}$$

En lo que resta del capitulo se considerará un $n \in \mathbb{N}$ fijo y números arbitrarios $x, y \in \mathbb{Z}$. Lo anterior tiene como finalidad dar paso a establecer una relación entre elementos en $\mathbb{Z}$ por medio de los residuos al dividirse entre n.

Teorema 2.1. *Dos enteros x, y son **congruentes módulo** n, si y solo si, tienen el mismo residuo al dividirse entre n.*

Demostración. Suponga que $r \in \mathbb{N}$ es el residuo de y al dividirse entre n. Ahora, como $x \equiv y \bmod n$ se tiene que existe un entero $k \in \mathbb{Z}$ tal que $x - y = kn$. Por otro lado, $y = qn + r$ con $0 \leq r < n$. En consecuencia, $x = y + kn = qn + r + kn = (q + k)n + r$. Como $k + q \in \mathbb{Z}$ se concluye que r es el residuo de x al dividirse entre n.

Recíprocamente, suponga que x y y tiene el mismo residuo al dividirse por n. Por consiguiente, existen $q_1, q_2, r \in \mathbb{Z}$ con $0 \leq r < n$ tal que

$$x = q_1 n + r,$$

$$y = q_2 n + r.$$

En consecuencia, $x - y = q_1 n + r - q_2 n - r = q_1 n - q_2 n = (q_1 - q_2)n$ como $q_1, q_2 \in \mathbb{Z}$ entonces n divide a $x - y$ por tanto, $x \equiv y \pmod{n}$.

□

Teorema 2.2. *La congruencia módulo n es una relación de equivalencia sobre* $\mathbb{Z}$.

Demostración. Para esta prueba se deberá mostrar que la relación de congruencia es una relación de reflexiva, simétrica y transitiva. Considere $x, y, z \in \mathbb{Z}$.

1. Reflexiva. Como $n \mid 0 = x - x$, entonces $n \mid x - x$. Por tanto, $x \equiv x \pmod{n}$.

2. Simétrica. Suponga que $x \equiv y \pmod{n}$, por tanto se tiene que $n \mid (x - y)$ luego, $n \mid -(x - y) = y - x$ en consecuencia $y \equiv x \pmod{n}$.

3. Transitiva. Si $x \equiv y \pmod{n}$ y $y \equiv z \pmod{n}$ entonces $n \mid (x - y)$ y $n \mid (y - z)$. Ahora n divide a cualquier combinación lineal de $x - y$ y $y - z$, por tanto $n \mid (x - y) + (y - z) = x - z$ entonces $x \equiv z \pmod{n}$.

□

Con base en el Teorema 2.2 para cada $x \in \mathbb{Z}$ se define su clase de equivalencia bajo la relación de congruencia, como:

$$\overline{x} = \{m \in \mathbb{Z} : m \equiv x \mod n\} = \{m \in \mathbb{Z} : m = kn + x \text{ para un } k \in \mathbb{Z}\}. \tag{2}$$

Ahora, usando el algoritmo de la división, $x = nq + r$ con q y $r \in \mathbb{Z}$ y $0 \leq r \leq n-1$. Luego, $x - r = nq$ entonces $x \equiv r \pmod{n}$ y por lo tanto, $\overline{x} = \overline{r}$. En conclusión, solo existen n clases de equivalencia y estas tienen como representante a un residuo módulo n. Dicho lo anterior, se define al conjunto de clases de equivalencia o conjunto cociente $\mathbb{Z}/n\mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}. \tag{3}$$

Lo previamente descrito permite establecer la siguiente definición

Definición 2.2 (Conjunto $\mathbb{Z}_n$)**.** Sea $n \in \mathbb{N}$. Se define a $\mathbb{Z}_n \subseteq \mathbb{N}$ como un sistema completo de representantes de la relación de congruencia. Dado por

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}. \tag{4}$$

2.2. $\mathbb{Z}_n$ como un subgrupo

Con la finalidad de proporcionar una operación entre elementos $\mathbb{Z}_n$, será necesario también definir una operación entre elementos de $\mathbb{Z}/n\mathbb{Z}$. Por ello se establecen las siguientes definiciones.

Definición 2.3 (Suma módulo n)**.** Sea $n \in \mathbb{N}$ y $x, y \in \mathbb{Z}_n$. Se define la suma módulo

$$x \oplus y = x + y - n\left\lfloor \frac{x+y}{n} \right\rfloor. \tag{5}$$

Note, que de la forma en la que se definió $x \oplus y$ corresponde con una manera analítica de definir el residuo modulo n. Es decir, $x \oplus y := x + y \pmod{n}$.

Definición 2.4 (Suma de clases módulo n)**.** Sea $n \in \mathbb{N}$ y $\overline{x}$ y $\overline{y} \in \mathbb{Z}_n$. La suma de clases de equivalencia de x y y, se define como la clase de equivalencia de $x + y$. Dicho de otra forma:

$$\overline{x} + \overline{y} = \overline{x+y}. \tag{6}$$

Ahora, considere la función $Z : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ dada por $Z(x) = \overline{x}$. Observe que Z es un isomorfismo. Inicialmente es claro que la función F es biyectiva. Además, también verifica que $F(x \oplus y) = F(x) + F(y) = \overline{x} + \overline{y}$, como se muestra a continuación:

$$F(x \oplus y) = F(x+y) = \overline{x + y - n\left\lfloor \frac{x+y}{n} \right\rfloor} = \overline{x} + \overline{y} - \overline{n\left\lfloor \frac{x+y}{n} \right\rfloor} = \overline{x} + \overline{y} + \overline{0} = \overline{x} + \overline{y}.$$

Por tanto, Z y Z^{-1} son isomorfismos y además, los conjuntos $\mathbb{Z}_n$ y $\mathbb{Z}/n\mathbb{Z}$ comparten la misma estructura algebraica con las operaciones de suma módulo n y la suma de clases, respectivamente. Dicho lo anterior, se considera el siguiente resultado.

Teorema 2.3. *El conjunto $\mathbb{Z}_n$ es un grupo abeliano.*

Demostración. Para esta prueba, inicialmente se probará que el par $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo abeliano y posterior a ello, usando el isomorfismo Z^{-1}, se verificarán las propiedades de grupo para el par $(\mathbb{Z}_n, \oplus)$. Con base en lo anterior, considere $n \in \mathbb{N}$ y $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}/n\mathbb{Z}$.

1. **Cerradura bajo** $(\oplus)$: Por el algoritmo de la división $x + y = nq + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r \leq n-1$ y en consecuencia $x + y \equiv r \pmod{n}$. Ahora, por el Teorema 2.1; $\overline{x+y} = \overline{r}$ y por lo tanto, $\overline{x+y} \in \mathbb{Z}/n\mathbb{Z}$. Luego, como $Z^{-1}(\overline{x+y}) \in \mathbb{Z}_n$, entonces $x \oplus y \in \mathbb{Z}_n$.

2. **Asociatividad bajo** $(\oplus)$: Para esta prueba se usará el hecho de la suma de números reales cumple la propiedad asociativa. Por tanto, considere las siguientes igualdades:

$$\begin{aligned}
\overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + \overline{y+z}, \\
&= \overline{x + (y+z)}, \\
&= \overline{(x+y) + z}, \\
&= (\overline{x+y}) + \overline{z}, \\
&= (\overline{x} + \overline{y}) + \overline{z}.
\end{aligned}$$

   En conclusión, $\overline{x} + (\overline{y} + \overline{z}) = (\overline{x} + \overline{y}) + \overline{z}$. Luego, se tiene que

$$\begin{aligned}
Z^{-1}(\overline{x} + \overline{y} + \overline{z}) &= Z^{-1}((\overline{x} + \overline{y}) + \overline{z}), \\
Z^{-1}(\overline{x}) \oplus Z^{-1}(\overline{y} + \overline{z}), &= Z^{-1}(\overline{x} + \overline{y}) \oplus Z^{-1}(\overline{z}), \\
x \oplus (y \oplus z) &= (x \oplus y) \oplus z.
\end{aligned}$$

3. **Elemento neutro bajo** $(\oplus)$: Considere el elemento $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$. Luego, para $x \in \mathbb{Z}_n$ se tiene que,

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{0+x} = \overline{x}.$$

Por lo tanto, $\overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x}$. Luego, se tiene que

$$Z^{-1}(\overline{x} + \overline{0}) = Z^{-1}(\overline{0} + \overline{x}) = Z^{-1}(\overline{x}),$$

$$x \oplus 0 = 0 \oplus x = x.$$

4. **Elemento inverso bajo** ($\oplus$): Tome el número $n - x$. En tal caso se obtiene que,

   a) $\overline{x} + \overline{n - x} = \overline{x + (n - x)} = \overline{n} = \overline{0}$,

   b) $\overline{n - x} + \overline{x} = \overline{(n - x) + x} = \overline{n} = \overline{0}$.

   Por consecuencia $\overline{x} + \overline{n - x} = \overline{n - x} + \overline{x} = \overline{0}$. Luego, se tiene que

$$Z^{-1}(\overline{x} + \overline{n - x}) = Z^{-1}(\overline{n - x} + \overline{x}) = Z^{-1}(\overline{0}),$$

$$x \oplus (n - x) = (n - x) \oplus x = 0.$$

5. **Conmutatividad bajo** ($\oplus$): Partiendo de la suma de números enteros cumple la propiedad conmutativa, considere las siguientes igualdades:

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}.$$

   Por lo tanto, $\overline{x} + \overline{y} = \overline{y} + \overline{x}$. Luego, tenemos que

$$Z^{-1}(\overline{x} + \overline{y}) = Z^{-1}(\overline{y} + \overline{x}),$$

$$x \oplus y = y \oplus x.$$

Con lo anterior se concluye que $(\mathbb{Z}_n, \oplus)$ es un grupo abeliano. □

Por otra parte, respecto a cuestiones de notación para esta sección, para cada $x, y \in \mathbb{Z}_n$, $x + y$ se representará la suma entre x y el inverso de y como $x \ominus y$. Entre otros aspectos, para cada $i \in \mathbb{Z}$ y $x \in \mathbb{Z}_n$ se

concluye que $ix \in \mathbb{Z}_n$. Puesto que, se define el producto ix como la suma modulo n de x consigo mismo, repetidamente, i-veces.

2.3. $\mathbb{Z}_n$ como espacio métrico

Ya establecidas las operaciones entre elementos de $\mathbb{Z}_n$, se da continuación a esta sección enunciado la forma en la que se medirá la distancia entre elementos de $\mathbb{Z}_n$.

Definición 2.5 (Función medida)**.** Sea $n \in \mathbb{N}$ y $x, y \in \mathbb{Z}_n$. Se define la función $\delta : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{R}$ dada por $\delta(x, y) = |x \ominus y|_n$, donde $|z|_n = min\{z, n - z\}$ para $z \in \{0, \ldots, n - 1\}$.

Observación 1. Considere $\delta(x, y) = min\{x \ominus y, n - (x \ominus y)\}$. Sabiendo que, $n - (x \ominus y) \equiv y \ominus x \pmod{n}$, es posible reinterpretar la función $\delta(x, y) = min\{x \ominus y, y \ominus x\}$.

Para establecer que δ corresponde a una función que mide correctamente la distancia entre elementos de $\mathbb{Z}_n$, es necesario y suficiente probar que δ es una métrica.

Teorema 2.4. *La función δ es una métrica.*

Demostración. Sea $x, y, z \in \mathbb{Z}_n$, se supone, sin pérdida de generalidad, que $\delta(x, y) = min\{y \ominus x, x \ominus y\} = x \ominus y$. Ahora, se mostrará que la función δ cumple las siguientes condiciones:

1. $\delta(x, y) \geq 0$.

   $\delta(x, y) = x \ominus y \in \mathbb{Z}_n = \{0, \ldots, n - 1\}$, entonces $\delta(x, y) \geq 0$.

2. $\delta(x, y) = 0$ si y solo si $x = y$.

   Sea $\delta(x, y) = x \ominus y = 0$. Como $x, y \in \mathbb{Z}_n$, entonces se deduce que $x \ominus y \in \{x - y, y - x\}$. Suponiendo, sin pérdida de generalidad, que $x \ominus y = x - y$, luego, $x - y = 0$ y por tanto, $x = y$.
   Por otro lado, si $x = y$ entonces $x - y = 0$. Por tanto, $x \ominus y = x - y - n\left\lfloor \frac{x-y}{n} \right\rfloor = 0 - n\left\lfloor \frac{0}{n} \right\rfloor = 0$. Lo cual concluye que, $x \ominus y = 0$.

3. $\delta(x, y) = \delta(y, x)$.

   Sea $\delta(y, x) = min\{y \ominus x, x \ominus y\} = x \ominus y = \delta(x, y)$.

4. $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$.

   Sin pérdida de generalidad suponga que $\delta(x, z) = min\{x \ominus z, z \ominus x\} = x \ominus z$ y que $\delta(y, z) = min\{y \ominus z, z \ominus y\} = y \ominus z$. Ya que, $x \ominus z \in \{x - z, z - x\}$ y $z \ominus y \in \{z - y, y - z\}$, entonces, suponga que $x \ominus z = x - z$ y $z \ominus y = z - y$. Ahora, considere las siguientes desigualdades:

$$0 \leq y - z,$$
$$0 \leq 2y - 2z,$$
$$x \leq 2y - 2z + x,$$
$$x - y \leq x - z + y - z,$$
$$x \ominus y \leq x \ominus z + y \ominus z,$$
$$\delta(x, y) \leq \delta(x, z) + \delta(y, z).$$

En conclusión, $(\mathbb{Z}_n, \delta)$ es un espacio métrico. □

2.4. Grafos y $\mathbb{Z}_n$

Para finalizar el capítulo, se enunciará una manera de interpretar al conjunto $\mathbb{Z}_n$ de forma geométrica, la cual será de utilidad al momento de probar algunos resultados sobre los conjuntos profundos de Erdős. Es así, que se considera la siguiente definición:

Definición 2.6. (Ciclo $\mathbb{C}_n$) Sea $n > 1$ y $\mathbb{C}_n = G(V, E_n)$ el grafo cíclico de n vértices y n aristas, donde el conjunto de vértices es $V = \mathbb{Z}_n = \{0, \ldots, n-1\}$ y el de aristas es $E_n = \{\{z, z+1\} : z \in V - \{n-1\}\} \cup \{n-1, 0\}$.

Note, que si $n \geq 3$, entonces el grafo anterior forma un polígono regular es decir, cada vértice se conecta con exactamente dos vértices. Dicho esto, la distancia entre dos vértices i y j del grafo $\mathbb{C}_n$, se define como la cantidad mínima de aristas comprendidas entre los dos vértices. Con esto se define la siguiente función distancia, tal y como hizo Toussaint (2013), denotándola como $d(i, j) = min\{|i - j|, n - |i - j|\}$. Seguidamente sabiendo que el par ordenado $(\mathbb{C}_n, d)$ corresponde con un espacio métrico se procede a mostrar la relación entre el conjunto $\mathbb{Z}_n$ y el grafo $\mathbb{C}_n$.

Teorema 2.5. *Los espacios métricos* $(\mathbb{Z}_n, \delta)$ *y* $(\mathbb{C}_n, d)$ *son isométricos.*

Demostración. Sea la función $\phi : \mathbb{Z}_n \to \mathbb{C}_n$ definida como $\phi(x) = x$, donde x corresponde con uno de los vértices del conjunto V. Ahora, se mostrará que $\delta(x, y) = d(\phi(x), \phi(y))$. Inicialmente, se sabe que $\delta(x, y) = min\{x \ominus y, n - (x \ominus y)\}$. Por otro lado, se tiene que

$$\begin{aligned} d(\phi(x), \phi(y)) &= min\{|\phi(x) - \phi(y)|, n - |\phi(x) - \phi(y)|\}, \\ &= min\{|x - y|, n - |x - y|\}. \end{aligned}$$

Como $|x - y| \in \{0, \ldots, n - 1\}$ se infieren los siguiente casos.

1. Si $0 < x - y < n - 1$, se tiene que $|x - y| = x - y = x \ominus y$, y por tanto,

$$\begin{aligned} d(\phi(x), \phi(y)) &= min\{|\phi(x) - \phi(y)|, n - |\phi(x) - \phi(y)|\}, \\ &= min\{|x - y|, n - |x - y|\}, \\ &= min\{x \ominus y, n - (x \ominus y)\}, \\ &= \delta(x, y). \end{aligned}$$

2. Si $0 > x - y > -(n - 1)$, entonces $0 < y - x < n - 1$ y por tanto, $|x - y| = y - x = y \ominus x$. Concluyendo que,

$$\begin{aligned} d(\phi(x), \phi(y)) &= min\{|\phi(x) - \phi(y)|, n - |\phi(x) - \phi(y)|\}, \\ &= min\{|x - y|, n - |x - y|\}, \\ &= min\{y \ominus x, n - (y \ominus x)\}, \\ &= \delta(y, x), \\ &= \delta(x, y). \end{aligned}$$

Por lo tanto, los espacios son isométricos. □

Ya establecidos, los preliminares del estudio, se procede a introducir el concepto y las caracterís-

ticas de los conjuntos profundos de Erdős o también llamados, en este estudio, 1-Familias profundas de Erdős. Cabe resaltar que como se trabajarán con elementos de $\mathbb{Z}_n$ se escribirá la operación suma modulo n entre elementos de $\mathbb{Z}_n$, dada por $x \oplus y$, simplemente como $x + y$.

3. Conjuntos Profundos de Erdős (caso s=1)

El propósito de esta sección es introducir algunos conceptos y resultados claves sobre los cuales se fundamenta este trabajo. Principalmente, se presentarán algunas definiciones que permiten establecer el concepto de familias profundas de Erdős en $\mathbb{Z}_n$.

En las definiciones de esta sección se considerará que: $x, y \in C \subseteq \mathbb{Z}_n$, donde $|C| > 1$.

Definición 3.1. (Multiconjunto de distancias) El multiconjunto de las distancias entre elementos distintos de C, se define como:

$$\Delta C = \{\delta(x, y) : \{x, y\} \subseteq C \wedge x \neq y\}. \tag{7}$$

Note que, la cantidad de distancias en ΔC debe ser $\binom{|C|}{2}$.

Definición 3.2 (Soporte de un multiconjunto)**.** El soporte de ΔC es el conjunto de todas las distancias diferentes en ΔC y se denota como $S(\Delta C)$.

Definición 3.3 (Multiplicidad de las distancias)**.** Sea $d \in S(\Delta C)$. La multiplicidad de la distancia d, denotada por $m(d, C)$, se define como:

$$m(d, C) = |\{\{x, y\} \subseteq C : x \neq y \wedge \delta(x, y) = d\}|. \tag{8}$$

Definición 3.4 (Conjunto de multiplicidades)**.** El conjunto de multiplicidades de ΔC se define como:

$$M(\Delta C) = \{m(d, C) : d \in S(\Delta C)\}. \tag{9}$$

Observación 2. En algunos textos el multiconjunto ΔC se escribe usando notación exponencial de la forma, $\Delta C = \{{d_1}^{m_1}, \ldots, {d_n}^{m_n}\}$, con $d_k \in S(\Delta C)$ y $m_k \in M(\Delta C)$, para $1 \leq k \leq n$.

Para mayor claridad, se desarrollará el siguiente ejemplo.

Ejemplo 3.1. Sea $C = \{1, 3, 5, 7\} \subseteq \mathbb{Z}_8$. Para calcular el multiconjunto de distancias $\Delta(C)$, se realizará una tabla, donde cada casilla indica la distancia entre dos elementos, $x, y \in C$, los cuales están posicionados en la primera fila y primera columna respectivamente, esto se observa en la Tabla 1. Puesto que, para $x, y \in \mathbb{Z}_8, \delta(x, y) = \delta(y, x)$ y $x \neq y$, entonces el multiconjunto de distancias, ΔC, consiste en todas las distancias por encima de la diagonal de la tabla. Es así, que en la Tabla 2, los números en la diagonal o por debajo de esta se omiten, siendo reemplazados por un punto ($\cdot$). lo anterior, se muestra a continuación:

Tabla 1

Distancias en ΔC

y \ x	1	3	5	7
1	0	2	4	2
3	2	0	2	4
5	4	2	0	2
7	2	4	2	0

Tabla 2

Distancias en ΔC

y \ x	1	3	5	7
1	$\cdot$	2	4	2
3	$\cdot$	$\cdot$	2	4
5	$\cdot$	$\cdot$	$\cdot$	2
7	$\cdot$	$\cdot$	$\cdot$	$\cdot$

Es así, que el multiconjunto de distancias corresponde con

$$\Delta C = \{2, 2, 2, 2, 4, 4\} = \{2^4, 4^2\}.$$

Igualmente, el soporte y conjunto de multiplicidades corresponden respectivamente a,

$$S(\Delta C) = \{2, 4\} \qquad y \qquad M(\Delta C) = \{2, 4\}.$$

A continuación, se definirá el primer objeto matemático de interés en este trabajo.

Definición 3.5 (Conjunto profundo de Erdős)**.** Sea $C \subseteq \mathbb{Z}_n$. Se dice que C es un **conjunto profundo de Erdős** si y solo si, para cada $i \in \{1, \ldots, k-1\}$, con $|C| = k$, existe una distancia d_i que satisface:

$$m(d_i, C) = |\{\{x, y\} \subseteq C : x \neq y \wedge \delta(x, y) = d_i\}| = i. \tag{10}$$

Observación 3. En otras palabras, el conjunto $C \subseteq \mathbb{Z}_n$ es profundo de Erdős, si se cumplen las siguientes dos condiciones:

1. La función $f : S(\Delta C) \to M(\Delta C)$, definida como $f(d) = m(d, C)$, es biyectiva.
2. $M(\Delta C) = \{1, \ldots, k-1\}$ con $k = |C|$.

El siguiente ejemplo complementa la definición anterior.

Ejemplo 3.2. Sea $C = \{0, 4, 5, 9, 10, 15\} \subseteq \mathbb{Z}_{16}$. Para determinar el multiconjunto de distancias, ΔC, se usará la siguiente tabla.

Tabla 3

Distancias en ΔC

x \ y	0	4	5	9	10	15
0	0	4	5	7	6	1
4	4	0	1	5	6	5
5	5	1	0	4	5	6
9	7	5	4	0	1	6
10	6	6	5	1	0	5
15	1	5	6	6	5	0

Es así, que:

$$\Delta(C) = \{7, 4, 4, 1, 1, 1, 6, 6, 6, 6, 5, 5, 5, 5, 5\} = \{7^1, 4^2, 1^3, 6^4, 5^5\}$$

Tal y como se observa en el multiconjunto ΔC, para cada $i \in \{1, \ldots, 5\}$, existe una d_i tal que la $m(d_i, C) = i$. Por tanto, C es un conjunto profundo de Erdős.

Para ser más rigurosos, se verifica el resultado anterior calculando, por definición, las multiplicidades de cada distancia en $S(\Delta C)$:

- $m(7, C) = |\{\{9, 0\}\}| = 1$,

- $m(4, C) = |\{\{9, 5\}, \{4, 0\}\}| = 2$,
- $m(1, C) = |\{\{5, 4\}, \{9, 10\}, \{15, 0\}\}| = 3$,
- $m(6, C) = |\{\{10, 0\}, \{10, 4\}, \{15, 5\}, \{15, 9\}\}| = 4$,
- $m(5, C) = |\{\{5, 0\}, \{9, 4\}, \{15, 4\}, \{10, 5\}, \{15, 10\}\}| = 5$.

Entre otros aspectos, el multiconjunto de distancias de un conjunto profundo de Erdős presenta la siguiente forma:

$$\Delta C = \{\delta(x, y) : \{x, y\} \subseteq C \wedge x \neq y\} = \{d_1^1, \ldots, d_{k-1}^{k-1}\}, \tag{11}$$

donde, $d_i \neq d_j$ para todo $i \neq j$. Al multiconjunto de distancias de un conjunto profundo de Erdős se le llamará, en este trabajo, **Multiconjunto de Erdős**. Con la meta de estudiar la clasificación de este tipo de subconjuntos de $\mathbb{Z}_n$ Gaede (2022) establece la siguiente definición.

Definición 3.6 (Progresiones aritméticas modulares)**.** Sea $g \in \mathbb{Z}_n$ y $k \in \mathbb{N}$. Se define una progresión aritmética modular en $\mathbb{Z}_n$ ó AP_n, como el conjunto:

$$AP(g, k, n) = \{ig : 0 \leq i \leq k - 1\} = \{0, g, \ldots, (k - 1)g\} \tag{12}$$

Definición 3.7 (traslación de una progresión aritmética)**.** Sea $a \in \mathbb{Z}_n$, se define la traslación de una progresión aritmética en $\mathbb{Z}_n$, $AP(g, k, n)$, como el conjunto:

$$a + AP(g, k, n) = \{a + ig : 0 \leq i \leq k - 1\} = \{a, a + g, \ldots, a + (k - 1)g\} \tag{13}$$

Ejemplo 3.3. Tomando $a = 1$, $g = 2$, $k = 4$ y $n = 7$, tenemos que $a + AP(g, k, n) = 1 + AP(2, 4, 7) = \{1 + 2 \cdot (0), 1 + 2 \cdot (1), 1 + 2 \cdot (2), 1 + 2 \cdot (3)\} = \{1 + 0, 1 + 2, 1 + 4, 1 + 6\} = \{1, 3, 5, 0\}$. Luego el multiconjunto de distancias $\Delta(1 + AP(2, 4, 7)) = \{1, 3, 3, 2, 2, 2\} = \{1^1, 2^3, 3^2\}$, de donde se concluye que $1 + AP(g, k, n)$ es un conjunto profundo de Erdős.

Posterior a establecer la definición anterior, Gaede (2022) en su investigación estudia algunos resultados propuestos por Toussaint (2013) y los interpreta en el contexto de $\mathbb{Z}_n$. Entre ellos, se encuentra

el resultado principal de esta sección, el cual se le denominará, en este trabajo, como el Teorema de Caracterización de los Conjuntos Profundos de Erdős en $\mathbb{Z}_n$. Dicha caracterización está definida a partir de las progresiones aritméticas modulares. Es así, que para llegar a demostrar este resultado se debe recurrir a algunos elementos iniciales y a una diversidad de lemas sobre conjuntos profundos de Erdős que serán parte esencial de la construcción del teorema.

Sean $a, g \in \mathbb{Z}_n$ y $n, k \in \mathbb{N}$con $k, n > 1$ y la progresión aritmética modular, dada por $AP(g, k, n)$. Considerando $0 \leq j < i \leq k - 1$, se redefine el multiconjunto de distancias de A como:

$$\Delta(a + AP(g, k, n)) = \{\delta(ig, jg) : j < i\} = \{|(i - j)g|_n : j < i\}. \tag{14}$$

Lo anterior será de utilidad para la prueba de algunos resultados claves para la construcción del teorema de caracterización de los conjuntos profundos de Erdős en $\mathbb{Z}_n$. Entre ellos, el siguiente lema enuncia la relación entre el multiconjunto de distancias de un conjunto profundo de Erdős y el multiconjunto de distancias de una traslación de este.

Lema 3.1. *Sea $A \subseteq \mathbb{Z}_n$. A es un conjunto profundo de Erdős si y solamente si, para todo $a \in \mathbb{Z}_n$, la traslación $a + A$ es un conjunto profundo de Erdős.*

Demostración. Puesto que el conjunto $a + A = \{a + x : x \in A\}$, es posible redefinir el multiconjunto de distancias $\Delta(a + A)$ de la siguiente manera:

$$\begin{aligned}
\Delta(a + A) &= \{|a + x - (a + y)|_n : \{x, y\} \subseteq A \wedge x \neq y\}, \\
&= \{|x - y|_n : \{x, y\} \subseteq A \wedge x \neq y\}, \\
&= \{\delta(x, y) : \{x, y\} \subseteq A \wedge x \neq y\}, \\
&= \Delta A.
\end{aligned}$$

Como A es un conjunto profundo de Erdős y $\Delta A = \Delta(a + A)$, se tiene que $a + A$ es un conjunto profundo de Erdős. □

El siguiente lema establece el máximo del conjunto de multiplicidades para una progresión aritmética cuando esta corresponde a un conjunto profundo de Erdős.

Lema 3.2. *Sea $A = a + AP(g, k, n) \subseteq \mathbb{Z}_n$ un conjunto profundo de Erdős. El*

$$\max(M(\Delta A)) = m(d, A),$$

donde $d = \delta(a, a + g) = |g|_n$.

Demostración. Como A es un conjunto profundo de Erdős, por el Lema 3.1, se tiene que $\Delta A = \Delta AP(g, k, n)$. Luego, $M(\Delta A) = M(\Delta AP(g, k, n)) = \{1, \ldots, k-1\}$ y por tanto, $\max(M(\Delta A)) = k - 1$. Por otro lado, se sabe que

$$m(|g|_n, A) = |\{\{x, y\} \subseteq A : x \neq y \wedge \delta(x, y) = |g|_n\}|.$$

Ahora, se define el conjunto $D = \{\{ig, (i-1)g\} : 1 \leq i \leq k-1\}$. Note que $D \subseteq \{\{x, y\} \subseteq A : x \neq y \wedge \delta(x, y) = |g|_n\}$ y para cada $1 \leq i \leq k - 1$,

$$\delta(ig, (i-1)g) = |g|_n.$$

Es así, que $|D| \leq |\{\{ig, (i-1)g\} : 1 \leq i \leq k-1\}|$ y en consecuencia, $k - 1 \leq m(|g|_n, A)$. Por tanto, $\max(M(\Delta A)) \leq m(|g|_n, A)$ y dado que, $\max(M(\Delta A)) \geq m(|g|_n, A)$. Se concluye que $\max(M(\Delta A)) = m(d, A)$.

□

Los siguientes resultados se establecerán con la finalidad estudiar los diferentes aspectos y condiciones para los cuales una progresión aritmética corresponde a un conjunto profundo de Erdős en $\mathbb{Z}_n$. Inicialmente, el lema a continuación, establece que todo progresión aritmética, $AP(g_1, k, n) \subseteq \mathbb{Z}_n$, se puede interpretar como la traslación de otra progresión aritmética de la forma $a + AP(g_2, k, n)$, con $a \in \mathbb{Z}_n$. Esto, con el objeto de entender toda traslación de una progresión aritmética por medio de un subconjunto

propio de generadores en $\mathbb{Z}_n$.

Lema 3.3. *Sea $A = AP(g_1, k, n) \subseteq \mathbb{Z}_n$ una progresión aritmética, entonces existen $a,\ g_2 \in \mathbb{Z}_n$, con $1 \leq g_2 \leq \left\lfloor \frac{n}{2} \right\rfloor$, tales que $AP(g_1, k, n) = a + AP(g_2, k, n)$.*

Demostración. Se van a considerar dos casos:

1. Si $g_1 \leq \left\lfloor \frac{n}{2} \right\rfloor$, basta con tomar $g_2 = g_1$ y $a = 0$.

2. Si $\left\lfloor \frac{n}{2} \right\rfloor < g_1 \leq n - 1$, entonces $-\left\lfloor \frac{n}{2} \right\rfloor > g_1 \geq 1 - n$. Luego,

$$n - \left\lfloor \frac{n}{2} \right\rfloor > n - g_1 \geq 1,$$

$$n - \left\lfloor \frac{n}{2} \right\rfloor - 1 \geq n - g_1 \geq 1.$$

   Por otro lado, como $n \in \mathbb{N}$, se cumple que $\left\lfloor \frac{n}{2} \right\rfloor \geq n - \left\lfloor \frac{n}{2} \right\rfloor - 1$. Por tanto, $1 \leq n - g_1 \leq \left\lfloor \frac{n}{2} \right\rfloor$.

   Tomando $n - g_1 = g_2$, la progresión aritmética de tamaño k y generador g_2 es:

$$\begin{aligned} AP(g_2, k, n) &= AP(n - g_1, k, n), \\ &= \{(n - g_1)i : 0 \leq i \leq k - 1\}, \\ &= \{0, n - g_1, \ldots, (k - 1)(n - g_1)\}. \end{aligned}$$

   Ahora, considerando $a = (k - 1)g_1$, se tiene que:

$$\begin{aligned} a + AP(n - g_1, k, n) &= \{a + (n - g_1)i : 0 \leq i \leq k - 1\}, \\ &= \{(k - 1)g_1 + (n - g_1)i : 0 \leq i \leq k - 1\}, \\ &= \{kg_1 - g_1 + ni - g_1 i : 0 \leq i \leq k - 1\}, \\ &= \{ni + g_1(k - i - 1) : 0 \leq i \leq k - 1\}. \end{aligned}$$

Ya que, $ni \equiv 0 \pmod{n}$, entonces $ni + g_1(k-i-1) \equiv g_1(k-i-1) \pmod{n}$ y por tanto, se tiene que:

$$a + AP(n - g_1, k, n) = \{g_1(k-i-1) : 0 \leq i \leq k-1\}$$

Luego, como $0 \leq i \leq k-1$, entonces $0 \leq k-i-1 \leq k-1$. Llamando $j = k-i-1$, se concluye que:

$$\begin{aligned} a + AP(n - g_1, k, n) &= \{g_1 j : 0 \leq j \leq k-1\} \\ &= AP(g_1, k, n) \end{aligned}$$

Por lo tanto, $a + AP(n - g_1, k, n) = a + AP(g_2, k, n) = AP(g_1, k, n)$.

□

El siguiente lema establece un limite en el tamaño del soporte del multiconjunto de distancias de un subconjunto en $\mathbb{Z}_n$. Considerando a $\mathbb{Z}_n$ como grupo y dado que $g \in \mathbb{Z}_n$. El subgrupo de $\mathbb{Z}_n$ generado por el elemento g, será denotado por $\langle g \rangle$. Entre otros aspectos, también será necesario considerar la definición del orden de $\langle g \rangle$, escrito como $|g|$ y satisface que $|g| = \frac{n}{\gcd(n,g)}$ [1].

El siguiente resultado será de gran utilidad al momento de demostrar el Teorema de Caracterización de los Conjuntos Profundos de Erdős.

Lema 3.4. *Sea $g \in \mathbb{Z}_n$ y $C \subseteq \langle g \rangle$, entonces $|S(\Delta C)| \leq \left\lfloor \frac{|g|}{2} \right\rfloor = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$.*

Demostración. Sea $C \subseteq \langle g \rangle = \{mg : 0 < m \leq |g|\}$ y defina

$$L_g = \left\{ ig : 0 \leq i \leq \left\lfloor \frac{|g|}{2} \right\rfloor \right\} \qquad y \qquad L_g^{-1} = \left\{ jg : \left\lfloor \frac{|g|}{2} \right\rfloor \leq j \leq |g| \right\}.$$

Note que $\langle g \rangle = L_g \cup L_g^{-1}$. Se mostrará que si $x \in L_g$, entonces $-x \in L_g^{-1}$. Para ello, se van a considerar los siguientes casos:

[1] $\gcd(n, g)$ denota al máximo común divisor entre n y g.

Caso 1: Suponga que $x = mg \in L_g$ es su propio inverso, entonces $x + x = 0$, por tanto, $2mg = 0$. Luego, $|g|$ divide a $2m$. Puesto que, $0 \leq m \leq \left\lfloor \frac{|g|}{2} \right\rfloor$, entonces $0 \leq 2m \leq 2\left\lfloor \frac{|g|}{2} \right\rfloor \leq |g|$, es decir $|g|$ divide a $2m$ y $0 \leq 2m \leq |g|$. De lo cual, se deduce que, $2m = 0$ ó $2m = |g|$, entonces $m = 0$ ó $\frac{|g|}{2}$, si $|g|$ es par. Por lo anterior, se concluye que $x = 0$ ó $x = \frac{|g|}{2}$, si $|g|$ es par.

De allí que, $x \in L_g^{-1}$. **Caso 2:** Suponga que x no es su propio inverso. Considere $x = ig$, con $0 < i < \left\lfloor \frac{|g|}{2} \right\rfloor$. Suponga que $-x \notin L_g^{-1}$. Ya que, $-x \in \langle g \rangle = L_g \cup L_g^{-1}$, entonces $-x \in L_g$, por tanto, $-x = i_1 g$ con $0 < i_1 < \left\lfloor \frac{|g|}{2} \right\rfloor$. Luego, $x + (-x) = ig + i_1 g = (i + i_1)g = 0$, lo cual implica que, $|g|$ divide a $(i + i_1)$. No obstante, como $0 < i_1, i < \left\lfloor \frac{|g|}{2} \right\rfloor$, entonces $i + i_1 < 2\left\lfloor \frac{|g|}{2} \right\rfloor \leq |g|$. Por tanto, $|g|$ no divide a $i + i_1$, lo cual contradice la proposición inicial. En conclusión, $-x \in L_g^{-1}$. Por otro lado, considere $|g|$ impar y $x = \left\lfloor \frac{|g|}{2} \right\rfloor g$. Luego, $-x = \left(|g| - \left\lfloor \frac{|g|}{2} \right\rfloor\right) g$ y $\left\lfloor \frac{|g|}{2} \right\rfloor < |g| - \left\lfloor \frac{|g|}{2} \right\rfloor$, entonces $-x \in L_g^{-1}$.

El resultado anterior será de utilidad para probar que

$$S\left(\Delta L_g\right) = S\left(\Delta L_g^{-1}\right).$$

Sea $d \in S\left(\Delta L_g\right)$ y $\Delta L_g = \left\{|(i - i_1)g|_n : 0 \leq i_1 < i \leq \left\lfloor \frac{|g|}{2} \right\rfloor\right\}$. Como, $i_1 < i$, entonces $1 \leq i - i_1 \leq \left\lfloor \frac{|g|}{2} \right\rfloor\}$. Llamando $t = i - i_1$, se tiene que

$$S\left(\Delta L_g\right) = \left\{|tg|_n : 1 \leq t \leq \left\lfloor \frac{|g|}{2} \right\rfloor\right\}. \tag{15}$$

Es así que, $d = |tg|_n$ para algún $t \in \left\{1, \ldots, \left\lfloor \frac{|g|}{2} \right\rfloor\right\}$. Luego, como $|tg|_n = |-tg|_n$ y $-tg \in L_g^{-1}$, entonces $d \in S\left(\Delta L_g^{-1}\right)$. La demostración de $S\left(\Delta L_g^{-1}\right) \subseteq S\left(\Delta L_g\right)$, es análoga al caso anterior. Por lo tanto, $S\left(\Delta L_g\right) = S\left(\Delta L_g^{-1}\right)$.

Del mismo modo, será indispensable para esta prueba, mostrar que

$$S\left(\Delta \langle g \rangle\right) \subseteq S\left(\Delta L_{\langle g \rangle}\right).$$

Por ello, considere $d \in S\left(\langle g \rangle\right)$, entonces existe $i_1 g, i_2 g \in \langle g \rangle$ con $i_1 > i_2$, tal que $d = \delta(i_1 g, i_2 g) = |i_1 g - i_2 g|_n = |(i_1 - i_2)g|_n$. Luego, independientemente de que, $1 \leq i_1 - i_2 \leq \left\lfloor \frac{|g|}{2} \right\rfloor$ ó $\left\lfloor \frac{|g|}{2} \right\rfloor < i_1 - i_2 \leq |g|$ se

tiene que, como $S\left(\Delta L_g\right) = S\left(\Delta L_g^{-1}\right)$, entonces $d \in S\left(\Delta L_g\right)$, en consecuencia $S\left(\Delta\langle g\rangle\right) \subseteq S\left(\Delta L_{\langle g\rangle}\right)$; lo cual implica que $|S\left(\Delta\langle g\rangle\right)| \leq \left|S\left(\Delta L_g\right)\right|$.

Con base en los resultados previos, para $C \subseteq \langle g\rangle$ se tiene que $S(\Delta C) \subseteq S\left(\Delta\langle g\rangle\right) \subseteq S\left(\Delta L_g\right)$, de ahí que $|S(\Delta C)| \leq \left|S\left(\Delta L_g\right)\right|$.

Para finalizar la prueba, resta demostrar que

$$\left|S\left(\Delta L_g\right)\right| = \left\lfloor \frac{|g|}{2} \right\rfloor.$$

De la igualdad (15), es de esperarse que en $S(\Delta L_g)$ hayan $\left\lfloor \frac{|g|}{2} \right\rfloor$ distancias. Por está razón, se probará que, para $1 \leq p, q \leq \left\lfloor \frac{|g|}{2} \right\rfloor$, si $|gp|_n = |gq|_n$ entonces $p = q$.

Sean $1 \leq p, q \leq \left\lfloor \frac{|g|}{2} \right\rfloor$, tales que $|gp|_n = |gq|_n$, entonces $gp = gq$ ó $gp = -gq$. Si $gp = gq$, entonces $(p-q)g = 0$. Lo cual implica que, $|g|$ divide a $(p-q)$ ó $p - q = 0$. Si $|g|$ divide a $(p-q)$, entonces $|g| \leq p - q$. Sin embargo, puesto que $-\left(\left\lfloor \frac{|g|}{2} \right\rfloor - 1\right) \leq p - q \leq \left\lfloor \frac{|g|}{2} \right\rfloor - 1$, entonces $p - q < \left\lfloor \frac{|g|}{2} \right\rfloor < |g|$, por tanto, este caso no es posible. De ahí que, $p - q = 0$, esto es $p = q$.

Si $gp = -gq$, entonces $(p+q)g = 0$. Lo cual implica que $|g|$ divide a $(p+q)$ ó $p + q = 0$. Si $|g|$ divide a $(p+q)$, entonces $|g| \leq p + q$. Luego, como $1 \leq q \leq \left\lfloor \frac{|g|}{2} \right\rfloor$ se tiene que, $-\left\lfloor \frac{|g|}{2} \right\rfloor \leq -q \leq -1$ y así, $-\left\lfloor \frac{|g|}{2} \right\rfloor \leq p \leq -1$. No obstante, $1 \leq p \leq \left\lfloor \frac{|g|}{2} \right\rfloor$; por tanto, este caso no es posible. Es así que, $|g|$ divide a $(p+q)$, entonces $|g| \leq (p+q)$. Luego, $2 \leq p + q \leq 2\left\lfloor \frac{|g|}{2} \right\rfloor$. Ahora, si $|g|$ es impar, entonces $2\left\lfloor \frac{|g|}{2} \right\rfloor < |g|$, lo cual implica que, $p + q < |g|$. Por ende, este caso no es posible. Si $|g|$ es par, entonces $2\left\lfloor \frac{|g|}{2} \right\rfloor = 2\frac{|g|}{2} = |g|$, lo cual implica que, $p + q \leq |g|$. En consecuencia, $p + q = |g|$, como $1 \leq p, q \leq \left\lfloor \frac{|g|}{2} \right\rfloor$, la única posibilidad es que $p = q = \frac{|g|}{2}$.

Por lo tanto, $\left|S\left(\Delta L_g\right)\right| = \left\lfloor \frac{|g|}{2} \right\rfloor$.
Finalmente, como $|S(\Delta C)| \leq \left|S\left(\Delta L_g\right)\right| = \left\lfloor \frac{|g|}{2} \right\rfloor = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$. Se concluye que $|S(\Delta C)| \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$. □

Ahora, para cualquier progresión aritmética $AP(g,k,n) \subseteq \langle g\rangle$, por el Lema anterior, $|S(\Delta AP(g,k,n))| \leq \left\lfloor \frac{|g|}{2} \right\rfloor = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$. Cuando $k = \left\lfloor \frac{|g|}{2} \right\rfloor + 1 = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$ se tendrá el menor valor de k para el cual $|S(\Delta AP(g,k,n))| = \left\lfloor \frac{|g|}{2} \right\rfloor$, es por ello, que se considerará un tamaño de $2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$.
Por otro lado, el siguiente resultado estudiará las traslaciones de una progresión aritmética y cuantas tiene

cada una de ellas.

Lema 3.5. *Sea $A = AP(g,k,n)$, con $2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. $A \neq \left\{0, \frac{n}{2}\right\}$ si y solo si A tiene n traslaciones distintas.*

Demostración. Primero se probará que si A tiene n traslaciones distintas entonces $A \neq \left\{0, \frac{n}{2}\right\}$, para ello suponga que $A = \left\{0, \frac{n}{2}\right\}$. Puesto que, A tiene n traslaciones distintas, entonces para todo $a_1, a_2 \in \mathbb{Z}_n$, con $a_1 \neq a_2$, se tiene que $a_1 + A \neq a_2 + A$. Sin embargo, tomando $a_1 = 0$ y $a_2 = \frac{n}{2}$, tenemos que

$$a_2 + A = \frac{n}{2} + \left\{0, \frac{n}{2}\right\} = \left\{\frac{n}{2}, n\right\} = \left\{0, \frac{n}{2}\right\} = 0 + \left\{0, \frac{n}{2}\right\} = 0 + A = a_1 + A.$$

Lo cual contradice que A tiene n traslaciones distintas, por lo tanto, $A \neq \left\{0, \frac{n}{2}\right\}$.

Recíprocamente, probemos que si $A \neq \left\{0, \frac{n}{2}\right\}$ entonces A tiene n traslaciones distintas. Sea $A = (g,k,n)$ con $g \neq \frac{n}{2}$. Suponga que A no tiene n traslaciones distintas, entonces existe un $a \in \mathbb{Z}_n$, con $0 < a < n$, tal que $a + A = A$.

Observe que $-a, a \in A$. En efecto, dado que, $a \in a + A$, entonces $a \in A$. Luego, como $0 \in A$, se tiene que $0 \in a + A$. Lo anterior implica que, existe un $0 < i \leq k - 1$, tal que $a + ig = 0$, en consecuencia $-a = ig$. Por tanto, $-a \in A$.

Por otro lado, se tiene que $a \in A \subseteq L_g$. Luego, como a es el inverso de $-a \in A$, entonces $a \in L_g^{-1}$. Por tanto, $a \in L_g \cap L_g^{-1} = \left\{0, \left\lfloor \frac{|g|}{2} \right\rfloor g\right\}$, como $a > 0$, entonces $a = \left\lfloor \frac{|g|}{2} \right\rfloor g$. Note que $|g|$ es par, pues en caso contrario se tiene que $-a = \left(|g| - \left\lfloor \frac{|g|}{2} \right\rfloor\right) g$, de donde $-a \notin L_g$, lo cual no es posible. Así que $|g|$ es par y $a = \frac{|g|}{2} g$. Lo cuál implica que, $k = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 = \left\lfloor \frac{|g|}{2} \right\rfloor + 1$ y n es par.
Luego, como $a = \frac{|g|}{2} g = \frac{n}{2} \frac{g}{\gcd(g,n)}$ y $\left|\frac{n}{2}\right| = 2$, entonces

$$a \equiv 0 \pmod{n} \qquad \text{ó} \qquad a \equiv \frac{n}{2} \pmod{n}.$$

Puesto que, $a \neq 0$, se tiene que $a = \frac{n}{2}$.

Ahora, como $A = \frac{n}{2} + A$, entonces para cada $0 \leq i \leq \frac{|g|}{2}$, existe un único $0 \leq j \leq \frac{|g|}{2}$, tal que $ig + \frac{n}{2} = jg$. Lo cual implica que, $2(i-j)g = n$, por ende $2(i-j)g = 0$ en $\langle g \rangle$.

Esto implica, que $2(i-j) = 0$ ó $|g|$ divide a $2(i-j)$. Si $2(i-j) = 0$, entonces $i = j$, en tal caso, como $ig + \frac{n}{2} = jg$, se concluye que $\frac{n}{2} = 0$, lo cual no posible.

Es así, que $|g|$ divide a $2(i-j)$ y por tanto, $|g| \leq 2(i-j)$. Luego, como $-\frac{|g|}{2} \leq i - j \leq \frac{|g|}{2}$, la única posibilidad es que $i - j = \frac{|g|}{2}$ y así, $i = \frac{|g|}{2} + j$.

Ya que, $0 \leq j \leq \frac{|g|}{2}$, entonces para todo i, se tiene que $j = 0$. Puesto, que para cada i, se corresponde con un único j, entonces solo puede existir un índice i. Ya que $j = 0$, entonces $i = 1$.

Con base en lo anterior, se tiene que $\frac{|g|}{2} = 1$, entonces $|g| = 2$ en $\langle g \rangle$, de lo cual se deduce que $g = \frac{n}{2}$. Esto contradice que $A \neq \left\{0, \frac{n}{2}\right\}$. Por lo tanto, A tiene n rotaciones distintas. □

Observación 4. La prueba anterior, exhibe que si existe un conjunto A que no tiene n traslaciones, entonces $A = AP\left(\frac{n}{2}, 2, n\right)$ y tendrá $\frac{n}{2}$ traslaciones distintas. En caso contrario, A tendrá n traslaciones distintas, una por cada $a \in \mathbb{Z}_n$.

A continuación, se presentarán los primeros resultados sobre progresiones aritméticas modulares, cuando estas corresponden a conjuntos profundos de Erdős en $\mathbb{Z}_n$. Para ello, será necesario establecer la operación de suma entre multiconjuntos. Sean ΔC_1 y ΔC_2 multiconjuntos de distancias, entonces

$$\Delta C_1 \uplus \Delta C_2 = \{d^{m(d,C_1)+m(d,C_2)} : d \in S(\Delta C_1) \cup S(\Delta C_2)\}.$$

Lema 3.6. *Sea $g = 1$; $2 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$ y $a \in \mathbb{Z}_n$, entonces $A = a + AP(1, k, n)$ es un conjunto profundo de Erdős.*

Demostración. Sea $A^* = AP(1, k, n) = \{0, 1, \ldots, k-1\}$. Para todo $x, y \in A^*$, tal que $y < x$, el multiconjunto ΔA^* se define como:

$$\Delta A^* = \{\delta(x, y) : y < x\}.$$

Como $0 \leq x, y \leq k - 1 \leq \left\lfloor \frac{n}{2} \right\rfloor$, entonces $0 < x - y \leq \left\lfloor \frac{n}{2} \right\rfloor$. Lo cual implica que $n - \left\lfloor \frac{n}{2} \right\rfloor \leq n - (x - y)$, y se tiene que

$$0 < x - y \leq \left\lfloor \frac{n}{2} \right\rfloor \leq n - \left\lfloor \frac{n}{2} \right\rfloor \leq n - (x - y).$$

Por tanto, $\delta(x, y) = min\{x - y, n - (x - y)\} = x - y$. En consecuencia,

$$\Delta A^* = \{x - y : y < x\}.$$

Ahora, para cada $w \in A^* - \{0\}$, se define el multiconjunto

$$\begin{aligned}\Delta w &= \{\delta(w, i) : 0 \leq i \leq w - 1\}\},\\ &= \{w - i : 0 \leq i \leq w - 1\},\\ &= \{t : 1 \leq t \leq w\}\},\\ &= \{1, \ldots, w\}.\end{aligned}$$

Note que $S(\Delta w) = \{1, \ldots, w\}$ y $M(\Delta w) = \{1\}$.

En particular, si $w_0 = \max(A^*) = k - 1$, entonces $\Delta w = \{1, \ldots, k - 1\}$, de donde $S(\Delta w) = \{1, \ldots, k - 1\}$ y $|S(\Delta w)| = k - 1$.

Ahora, veamos que $S(\Delta w_0) = S(\Delta A^*)$. Como $w_0 \in A^*$, se tiene que $S(\Delta w_0) \subseteq S(\Delta A^*)$. Por otra parte, tome $d \in S(\Delta A^*)$, entonces existe $x, y \in A^*$, con $y < x$, tal que $\delta(x, y) = x - y = d$. Luego, considere $z \in A^*$, con $z = w_0 - (x - y)$, entonces $z \leq w_0$. Luego, dado que $\delta(w_0, z) \in S(\Delta w)$ y $\delta(w_0, z) = w_0 - z = w_0 - (w_0 - (x - y)) = x - y = d$, se concluye que $d \in S(\Delta w_0)$. Por ende, $|S(\Delta w_0)| = |S(\Delta A^*)|$ y por tanto, $|S(\Delta A^*)| = k - 1$.

Finalmente, para probar que A^* es un conjunto profundo de Erdős, se mostrará que para toda $d \in S(\Delta A^*)$

$$m(d, A^*) = k - d. \tag{16}$$

Note que, cada distancia $d \in S(\Delta A^*)$, es resultado de una operación entre dos elementos $x, y \in A^*$

con $y < x$, por tanto, se deduce que

$$\Delta A^* = \biguplus_{w=1}^{k-1} \Delta w.$$

Dicho esto, para probar (16) es necesario y suficiente, encontrar todos los $w \in A^* - \{0\}$, tal que $d \in S(\Delta w)$. Luego, como $S(\Delta w) = \{1, \ldots, w\}$, se tiene que $d \in S(\Delta w)$, si y solo si $d \leq w$. Por tanto

$$\begin{aligned} m(d, A^*) &= |\{w : d \leq w \wedge w \in A - \{0\}\}|, \\ &= |\{w : d \leq w \wedge 1 \leq w \leq k-1\}|, \\ &= k - 1 - (d-1), \\ &= k - d. \end{aligned}$$

Además,

$$1 \leq d \leq k-1,$$

$$1 - k \leq -d \leq -1,$$

$$1 \leq k - d \leq k - 1,$$

lo cual concluye que $M(\Delta A^*) = \{1, \ldots, k-1\}$.

Por otro lado, sean $d_1, d_2 \in S(\Delta A^*)$, si $k - d_1 = k - d_2$, entonces $d_1 = d_2$. Por ello, la multiplicidad de cada elemento del soporte es única.

Por consiguiente, se concluye que $A^* = AP(1, k, n)$ es un conjunto profundo de Erdős. Luego, por el Lema 3.1 para cualquier $a \in \mathbb{Z}_n$, $a + AP(1, k, n)$ también es un conjunto profundo de Erdős. □

Lema 3.7. *Sea* $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, $2 \leq k \leq \left\lfloor \frac{n}{(2\text{gcd}(n,g))} \right\rfloor + 1$ *y* $a \in \mathbb{Z}_n$, *entonces,* $A = a + AP(g, k, n)$ *es un conjunto profundo de Erdős.*

Demostración. Sea $A_0 = AP(g, k, n)$ y $\Delta(A_0) = \{|(i-j)g|_n : i > j\}$. Puesto que, $0 \leq i, j \leq k-1$ con $j < i$,

entonces $1 \leq i - j \leq k - 1$. Llamando $t = i - j$, se tiene que

$$S(\Delta A_0) = \{|tg|_n : 1 \leq t \leq k - 1\}.$$

Luego, con base en la igualdad (15) de la demostración del Lema 3.4, se tiene que $|S(\Delta A_0)| = k-1$. Por otra parte, con base en el Lema 3.6, $A^* = AP(1, k, n)$ es un conjunto profundo de Erdős, tal que

$$S(\Delta A^*) = \{1, \ldots, k - 1\}.$$

Lo anterior, permite deducir que $|S(\Delta A_0)| = |S(\Delta A^*)|$.

Ahora, para todo $d \in S(\Delta A^*)$, se define

$$Q_1(d) = \{\{x, y\} \subseteq A^* : y < x \wedge x - y = d\}$$

y para todo $|dg|_n \in S(\Delta A_0)$, con $1 \leq d \leq k - 1$, se define

$$Q_g(dg) = \{\{xg, yg\} \subseteq A_0 : y < x \wedge |(x - y)g|_n = |dg|_n\}.$$

Seguidamente, por definición de multiplicidad, se tiene que

$$m(d, A^*) = |Q_1(d)| \qquad \text{y} \qquad m(|dg|_n, A_0) = |Q_g(|dg|_n)|.$$

Dicho lo anterior, para mostrar que A_0 es un conjunto profundo de Erdős, como A^* ya es un conjunto profundo de Erdős y $|S(\Delta A_0)| = |S(\Delta A^*)|$, será suficiente con probar que $m(d, A^*) = m(|dg|_n, A_0)$, para todo $d \in S(\Delta A^*)$.

Considere la función $\phi : Q_1(d) \to Q_g(|dg|_n)$, definida por $F(\{x, y\}) = \{xg, yg\}$, y probemos que ϕ es biyectiva.

ϕ es inyectiva: Sean $\{x_1, y_1\}, \{x_2, y_2\} \in Q_1(d)$ y supongamos que, $\phi(\{x_1, y_1\}) = \phi(\{x_2, y_2\})$, entonces $\{gx_1, gy_1\} = \{gx_2, gy_2\}$. Sin pérdida de generalidad podemos considerar que $gx_1 = gx_2$ y $gy_1 = gy_2$. Luego,

como $0 \leq x, y \leq k-1 = \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$, $(x_1 - x_2)g = 0$ y $(y_1 - y_2)g = 0$, entonces $x_1 = x_2$ y $y_1 = y_2$. Por tanto, ϕ es inyectiva.

ϕ **es sobreyectiva:** Sea $\{xg, yg\} \in Q_g(|dg|_n)$ y considere el conjunto $\{x, y\}$. Puesto que $\delta(xg, yg) = |(x-y)g|_n = |dg|_n$ y como $1 \leq x - y \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$, se tiene que $x - y = d$. Por tanto, $\{x, y\} \in Q_1(d)$, es así que $\phi(\{x, y\}) = \{xg, yg\}$. En conclusión, ϕ es sobreyectiva.

Por consiguiente, dado que ϕ es biyectiva y como $Q_1(d)$ y $Q_g(|dg|_n)$ son finitos, se tiene que $|Q_1(d)| = |Q_g(|dg|_n)|$. Lo cual implica que $m(d, A^*) = m(|dg|_n, A_0)$, por tanto, A_0 es un conjunto profundo de Erdős. Finalmente, por el Lema 3.1, el conjunto $A = a + AP(g, k, n)$ es un conjunto profundo de Erdős. □

El Lema 3.7, pone en evidencia que, bajo ciertas condiciones especificas para los parámetros g, k, el conjunto $a+AP(g, k, n)$ es un conjunto profundo de Erdős. El Teorema 3.10 complementa dicho lema de manera recíproca, estableciendo así el teorema de caracterización de los conjuntos profundos de Erdős en $\mathbb{Z}_n$. La prueba de este resultado se apoyará en el Teorema 2.5, donde se establece que $\mathbb{Z}_n$, con la métrica δ, es isométrico al ciclo $\mathbb{C}_n = (V, E)$, donde $V = \mathbb{Z}_n = \{0, \ldots, n-1\}$ y $E = \{\{z, z+1\} : z \in V - \{n-1\}\} \cup \{n-1, 0\}$ con la métrica d. Igualmente, será indispensable los siguiente resultados.

Lema 3.8. *Sea $x \in A \leq \mathbb{Z}_n$ y $0 < d \leq \left\lfloor \frac{n}{2} \right\rfloor$, entonces existe a lo sumo dos números $x_1, x_2 \in \mathbb{Z}_n$, tal que*

$$\delta(x, x_1) = \delta(x, x_2) = d.$$

Demostración. Sea $x \in A \leq \mathbb{Z}_n$. considere la ecuación $|x-y|_n = d$. Luego, $x - y = \pm d$. De allí, se deducen dos casos; $x - y = d$ ó $x - y = -d$. Si $x - y = d$, entonces $y = x - d$, caso contrario, $y = x + d$. Por tanto, $x_1 = x + d$ y $x_2 = x - d$. □

Observación 5. El Lema 3.8 se traduce al contexto del $\mathbb{C}_n$ de la siguiente forma. Sea v un vértice en $\mathbb{C}_n$ y $0 < d_0 \leq \left\lfloor \frac{n}{2} \right\rfloor$, entonces existen a lo sumo dos vértices, v_1 y v_2, tal que, $d(v, v_1) = d(v, v_2) = d_0$.

Lema 3.9. *Sea $A \leq \mathbb{Z}_n$ y $d \in S(\Delta A)$. Si $d \neq \frac{n}{2}$, entonces $m(d, \mathbb{Z}_n) = n$.*

Demostración. Considere el conjunto $\{i, i+d\} \subseteq \mathbb{Z}_n$, note que $\delta(i+d, i) = |i+d-i|_n = |d|_n = d$. Como $d \neq \frac{n}{2}$ por el Lema 3,5, el conjunto $\{i, i+d\}$ tiene n rotaciones distintas, es decir existen n conjuntos de la forma $\{a+i, a+i+d\}$, con $a \in \mathbb{Z}_n$, tal que $\delta(a+i, a+i+d) = d$. De allí, se deduce que $m(d, \mathbb{Z}_n) \geq n$. Suponga que $m(d, \mathbb{Z}_n) > n$, entonces existe un conjunto $\{i_1, j_1\}$, tal que $\delta(i_1, j_1) = d$ y $\{i_1, j_1\} \neq a + \{i, i+d\}$.

Ahora, considere $a_1 \in \mathbb{Z}_n$, tal que $a_1 + i_1 = i$. Como $\{i_1, j_1\} \neq a + \{i, i+d\}$ entonces, $a_1 + j_1 \neq (i+d)$ igualmente, $a_1 + j_1 \neq (i-d)$, pues caso contrario, $a_1 + \{i_1, j_1\} = \{a_1 + i_1, a_1 + j_1\} = \{i, i-d\} = -d + \{i, i+d\}$, lo cual no es posible, ya que $\{i_1, j_1\}$ no es traslación de $\{i, i+d\}$. Por lo anterior, se concluye que $i \in \mathbb{Z}_n$, existen 3 elementos distintos en $\mathbb{Z}_n$, tal que la distancia de estos al elemento i es d, lo cual contradice el Lema 3.8. Por tanto, $m(d, \mathbb{Z}_n) = n$. □

Teorema 3.10. *$C \subseteq \mathbb{Z}_n$ es un conjunto profundo de Erdős, si y solo si, para todo $a \in \mathbb{Z}_n$*

a. $C = a + \left\{0, \frac{n}{3}, \frac{2n}{3}, \frac{n}{6}\right\}$ *cuando* $n = 6t$, *con* $t \geq 1$, *ó*

b. $C = a + AP(g, k, n)$, *con* $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ *y* $k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$.

Demostración. Considere $C \subseteq \mathbb{Z}_n$, con $|C| = k$, un conjunto profundo de Erdős, entonces existe un $m \in S(\Delta C)$, tal que $m(m, C) = k - 1$.

Ahora, defina el grafo $G = (V(G), E(G))$; donde, el conjunto de vértices $V(G) = C$ y el conjunto de aristas corresponde con $E(G) = \{\{v, u\} : u, v \in C \wedge d(u, v) = m\}$. De la observación 5, para $u \in C$, existen a lo sumo $v_1, v_2 \in \mathbb{C}_n$, tal que

$$d(u, v_1) = d(u, v_2) = m.$$

Note, que si $v_1, v_2 \in C$, están dados por $v_1 = u + m$ y $v_2 = u - m$. De ahí, las posibles aristas con el vértice u en G, serían $\{u, u+m\}$ y $\{u, u-m\}$, por tanto no existen aristas múltiples y como $m > 0$, no existen bucles. Luego, con base en Syropoulos (2001), G es un grafo simple. Adicionalmente, como cada vértice tiene un grado menor o igual a 2, entonces G es la unión de ciclos y caminos simples

disjuntos. [2] Ahora, puesto que existen $k-1$ aristas y k vértices en G, entonces el grafo G consiste exactamente de un camino simple y algún número de ciclos.

Particularmente, cada ciclo de G corresponde con el subgrupo cíclico generado por $m \in \mathbb{Z}_n$ o una traslación de este. Es así que, cada ciclo tiene la misma cantidad de vértices, la cual es $r = \frac{n}{\gcd(m,n)}$ y una distancia entre vértices consecutivos de $m = \gcd(n, m)$. Note que m divide a n y $m \neq n$, caso contrario todo ciclo corresponde con $\mathbb{C}_n$, lo cual no es posible, ya que el camino y el ciclo no serían disjuntos.

Igualmente, ya que G es un grafo simple, cada ciclo debe tener al menos 3 vértices, es decir $r \geq 3$.

Es así, que la prueba se dividirá en 6 casos dependiendo de la longitud del camino y de cuantos ciclos tiene el grafo G. Se concluirá que los casos 1, 2, 4 y 5 son imposibles, el caso 3 implica la existencia del conjunto $C = a + \left\{0, \frac{n}{3}, \frac{2n}{3}, \frac{n}{6}\right\}$, cuando $n = 6t$ con $t \geq 1$ y el caso 6 concluirá que C corresponde con la traslación de una $AP(g, k, n)$.

Caso 1: G consiste de un camino simple de longitud 0 y ningún ciclo.

En tal caso, $G = \{x\}$, como $|C| > 2$, este caso no es posible.

Caso 2: G consiste de un camino simple de al menos longitud 1 y un solo ciclo.

Se mostrará que este caso es imposible, pues no existe una distancia con multiplicidad 1. Suponga que $G = (V(G), E(G))$ consiste del camino P_s con $s \geq 1$ y el ciclo C_r. Por otro lado, como C es un conjunto profundo de Erdős, entonces existen dos vértices, $v_1, v_2 \in C$, tal que la distancia $d_0 = d(v_1, v_2)$ cumple que $m(d_0, C) = 1$. Como $G = P_s \cup C_r$, se establecen los siguientes casos:

1. Suponga que v_1 y v_2 son vértices del C_r, entonces $v_1 + m$ y $v_2 + m$ también son vértices del C_r. Luego,

$$\begin{aligned} d(v_1 + m, v_2 + m) &= \delta(v_1, v_2) \\ &= min\{|v_1 + m - (v_2 + m)|_n, n - |v_1 + m - (v_2 + m)|_n\} \\ &= min\{|v_1 - v_2|_n, n - |v_1 - v_2|_n\} \\ &= \delta(v_1, v_2) = d(v_1, v_2) = d_0 \end{aligned}$$

[2] Se denotará, un camino de longitud s, con $s \leq 0$, como P_s y un ciclo de longitud r, con $r \leq 0$, como C_r. Dicha notación representa grafos arbitrarios, no especifica concretamente cuales son sus vértices correspondientes.

Por tanto, $m(d_0, C) > 1$. Lo cual contradice que C es un conjunto profundo de Erdős y por tanto, este caso no es posible.

2. Suponga que v_1 es un vértice del C_r y v_2 es un vértice de P_s. Como v_2, puede ser el extremo del camino, se tiene que: $v_1 - m$ y $v_2 - m$ son vértices del grafo G ó $v_1 + m$ y $v_2 + m$ son vértices del grafo G. Independientemente del caso, se sabe que $d(v_1 + m, v_2 + m) = d(v_1, v_2) = d_0$ y $d(v_1 - m, v_2 - m) = d(v_1, v_2) = d_0$. Por tanto, $m(d_0, C) > 1$. Lo cual contradice que C es un conjunto profundo de Erdős y por tanto, este caso no es posible.

3. Sea v_1 y v_2 vértices de P_s. Luego, v_1 y v_2 deben tener grado 1, caso contrario, $v_1 + m$ y $v_2 + m$, también serían vértices del camino y por tanto, $m(d_0, C) > 1$, lo cual no es posible. Como v_1 y v_2 tienen grado 1, entonces corresponden con el comienzo y el final del camino. Como el camino tiene s aristas, entonces $d(v_1, v_2) = \delta(v_1, v_2) = |sm|_n$. Por otro lado, considere v_3, un vértice de C_r, entonces $v_3 + sm$ es un vértice de C_r. Además, $d(v_3 + sm, v_3) = \delta(v_3 + sm, v_3) = |sm|_n$. Lo cual contradice que C es un conjunto profundo de Erdős y por tanto, este caso no es posible.
   Por lo tanto, el **caso 2** no es posible, es decir G no se puede representar como un camino simple de al menos longitud 1 y al menos un ciclo.

Caso 3: G consiste de un camino de longitud cero y un solo ciclo.

Para este caso se concluirá que $C = a + \left\{0, \frac{n}{3}, \frac{2n}{3}, \frac{n}{6}\right\}$ cuando $n = 6t$, con $t \geq 1$. Llame C_r al ciclo, P_0 al camino de longitud cero y x a su único vértice. Ahora, considere los siguientes casos en relación a m.

1. Suponga $m = \frac{n}{4}$, es decir, el ciclo tiene una distancia entre vértices de $\frac{n}{4}$. Puesto que P_0 y C_r son disjuntos, entonces la distancia de x a cualquier vértice de C_r es diferente a las distancias entre vértices de C_r, caso contrario, el vértice x pertenecería a C_r, lo cual no es posible. Luego, con base en la Observación 5, a lo sumo pueden existir dos vértices v_1 y v_2 en C_r, tal que $d(x, v_1) = d(x, v_2)$, de no ser así, todas las distancias entre los vértices de C_r y x serían distintas, de donde, las distancias entre x y los vértices de C_r poseen multiplicidad 1 ó 2. Como C_r tiene 4 vértices, se deduce que, existen

al menos dos distancias con multiplicidad 1 ó dos distancias con multiplicidad 2. Contradiciendo el hecho de que C es un conjunto profundo de Erdős. Por tanto, este caso no es posible.

2. Suponga que la distancia $m \neq \frac{n}{4}$. Note que no pueden existir dos distancias diferentes en el ciclo C_r. Como $V(C_r) = a + \langle m \rangle$ para algún $a \in \mathbb{Z}_n$, por el Lema 3.9 para cualquier $d \in S(a + \langle m \rangle)$, con $d \neq \frac{n}{2}$, se tiene que $m(d, a + \langle m \rangle) = r$, es decir, para la distancia m y $m' = |2m|_n = min\{2m, n - 2m\}$, se cumple que $m(m, a + \langle m \rangle) = m(m', a + \langle m \rangle)$. Por otro lado, para $v_1 \in a + \langle m \rangle$, $d(v_1, x) \neq m \neq m'$, caso contrario, x sería un vértice de C_r, lo cual no es posible. Como $C = a + \langle m \rangle \cup \{x\}$, entonces $m(m, C) = m(m', C)$. Puesto que C es un conjunto profundo de Erdős, entonces $m = m'$; de ahí $m = 2m$ ó $m = n - 2m$. El primer caso no es posible, ya que $m > 0$, por consiguiente, $m = n - 2m$, y así $m = \frac{n}{3}$. Esto implica que C_r, debe tener exactamente 3 vértices, es decir $r = 3$. Suponiendo que uno de los vértices de C_r es 0, entonces $V(C_r) = \left\{0, \frac{n}{3}, \frac{2n}{3}\right\}$.

   Dado que C es un conjunto profundo de Erdős y como G tiene 4 vértices, 3 vértices por el ciclo y 1 por el camino, entonces $M(\Delta C) = \{1, 2, 3\}$. Puesto que, $m(m, C) = 3$, entonces x debe estar a medio camino de dos de los tres vértices de C_r, pues de lo contrario, las distancias de x a los tres vértices de C_r serían distintas, por ende, habrían tres distancias con multiplicidad 1, lo cual no es posible. Igualmente, lo anterior obliga a n a ser par y por tanto, ser múltiplo de 6. Es así que, tomando x entre los vértices 0 y $\frac{n}{3}$, se tiene que $x = \frac{1}{2}\left(0 + \frac{n}{3}\right) = \frac{n}{6}$. Luego, por el Lema 3.1, para todo $a \in \mathbb{Z}_n$ el conjunto $a + \left\{0, \frac{n}{3}, \frac{2n}{3}, \frac{n}{6}\right\}$ es un conjunto profundo de Erdős.

Caso 4: G consiste de un camino simple de longitud 0 y más de un ciclo.

El objetivo de esta prueba será mostrar que este caso es imposible, pues existen al menos dos distancias con la misma multiplicidad.

Inicialmente, denoté al camino simple de longitud 0 por $P_0 = (\{x\}, \varnothing)$ y considere dos ciclos de longitud r dados por C_r y C'_r. Por otro lado, tome $v_1 \in V(C_r)$ y $v_2 \in V(C'_r)$, tal que $d(v_1, v_2) = d$, con d la menor distancia entre vértices de C_r y C'_r. Ya que los ciclos son disjuntos, entonces $d < m = \gcd(n, m)$. Por otro lado, como $r \geq 3$, entonces $n \geq 3\gcd(n, m)$ y por tanto, $\frac{n}{3} \geq \gcd(n, m)$.

Puesto que $\gcd(n, m) > d$, entonces $\frac{n}{3} > d$.

A continuación, se mostrará que $m(d, V(C_r) \cup V(C'_r)) = r$ ó $m(d, V(C_r) \cup V(C'_r)) = 2r$, para ello considere los siguientes casos:

Suponga que $d \neq \frac{m}{2}$. Ahora, para $0 \leq i \leq r-1$, $v_1 + im \in C_r$ y $v_2 + im \in C'_r$,

$$d(v_1 + im, v_2 + im) = |v_1 + im - (v_2 + im)|_n = |v_1 - v_2|_n = d.$$

Es así, que existen r conjuntos de la forma $\{v_1 + im, v_2 + im\}$, tal que $d(v_1 + im, v_2 + im) = d$. Luego, como $d \neq \frac{m}{2}$, entonces $d \neq m - d$. Esto implica, que para cada $v \in C_r$, existe un único $v' \in C'_r$, tal que $d(v, v') = d$. Por tanto, $m(d, V(C_r) \cup V(C'_r)) = r$.

Caso contrario, tomando $d = \frac{m}{2}$, defina el grafo $G' = (V(G'), E(G'))$, donde $V(G') = V(C_r) \cup V(C'_r)$ y $E(G') = \{\{u, v\} : d(u, v) = d\}$. Note que G' corresponde con el ciclo de $2r$ vértices, por tanto $m(d, V(C_r) \cup V(C'_r)) = 2r$. (Este caso ocurre cuando C_r es media traslación de C'_r).
Por otro lado, sean $v_1 + m, v_1 - m \in V(C_r)$ y $v_2 + m, v_2 - m \in V(C'_r)$. Como $d(v_1, v_2) = d$, entonces

$$d(v_2, v_1 + m) = |d - m|_n \qquad y \qquad d(v_1, v_2 + m) = |d + m|_n.$$

A partir de este punto se concentrarán los esfuerzos en estudiar las distancias d, $d' = |d + m|_n$ y $d'' = |d - m|_n$. Dado que los ciclos son disjuntos entonces, las distancias d, d' y d'' no pueden ocurrir como distancias entre vértices del mismo ciclo. Además, es sabido que x tiene una distancia d hasta un vértice $v \in V(C_r)$ si y solo si, x tiene una distancia d' al vértice $v + m$ e igualmente, $d(x, v) = d$ si y solo si, la distancia de x hasta el vértice $v - m$ es igual a d''. Asimismo ocurre si x fuese un vértice de otro ciclo distinto a C_r y C'_r. Por tal razón, el siguiente paso de esta prueba será determinar las multiplicidades de $|d - m|_n$ y $|d + m|_n$ en $V(C_r) \cup V(C'_r)$.

Puesto que, $d < m$, entonces $d(v_2, v_1 + m) = |d - m|_n = m - d$. Si $m - d \neq d$, entonces por cada vértice $v \in V(C_r)$ existe un único par de vértices $v_1, v_2 \in V(C'_r)$, tal que $d(v, v_1) = d$ y $d(v, v_2) = m - d = d''$. Por tanto, $m(d, V(C_r) \cup V(C'_r)) = m(d'', V(C_r) \cup V(C'_r)) = r$. Caso contrario si $m - d = d$, entonces $d = \frac{m}{2}$. A causa de esto $m(d, V(C_r) \cup V(C'_r)) = m(d'', V(C_r) \cup V(C'_r)) = 2r$.

Con respecto a la distancia $|m+d|_n$, se tendrá en consideración los siguientes casos: En primera instancia, suponga que $|m+d|_n \neq \frac{n}{2}$. Luego, independientemente de que $m-d \neq d$ ó $m-d=d$, se tiene que $m(d, V(C_r) \cup V(C'_r)) = m(|d-m|_n, V(C_r) \cup V(C'_r)) = m(|d+m|_n, V(C_r) \cup V(C'_r))$. Ya que, C es un conjunto profundo de Erdős se debe cumplir que $d = d' = d''$. Considerando, $d = d''$ entonces se tienen los siguiente casos: $d = d+m$ ó $d = n-(d+m)$. El primer caso no es posible, ya que $m > 0$ y del segundo se concluye que $2d + m = n$. Similarmente, si se asume que $d = d'$, entonces $2d' - m = n$. Finalmente, restando las dos ecuaciones $2d + m - (2d - m) = n - n$ se tiene que $2m = 0$. Lo cual no es posible, ya que inicialmente se estableció que $m > 0$. De esa forma se concluye que el caso es imposible.

Caso contrario, si $|m+d|_n = \frac{n}{2}$, entonces $d = m-d$, es decir $d = \frac{m}{2}$, pues si $d \neq |d-m|_n$ y como $d < m$, entonces $m(m, V(C_r)) = 2$, lo cual no es posible, pues $r \geq 3$. En consecuencia, $m(|d-m|_n, V(C_r) \cup V(C'_r)) = m(d, V(C_r) \cup V(C'_r)) = 2r$. Ahora, considere el grafo $C_{2r} = (V(C_{2r}), E(C_{2r}))$. Luego, como $|m+d|_n = \frac{n}{2}$ se tiene que $m(m+d, V(C_r)) \cup V(C'_r)) = \frac{2r}{2} = r$. Con base en lo anterior, se establece que el ciclo C_{2r}, corresponde con un ciclo de longitud 6. Puesto que, de no ser así, $|m+d|_n < \frac{n}{2}$, lo cual no es consistente con la suposición inicial. Luego, al tomar las distancias entre x y los vértices de los ciclos, se generarían 3 distancia distintas de multiplicidad 2 ó 6 distancias diferentes de multiplicidad 1. Note que, las distancias de x a los vértices de los ciclos son distintas a las distancias entre vértices de los ciclos, caso contrario, x sería vértice de uno de C_r ó C'_r, lo cual no es posible. Es decir, que existen al menos dos distancias distintas con misma multiplicidad. Lo cual contradice el hecho de que C es un conjunto profundo de Erdős.

Por lo tanto, no es posible, es decir G no se puede representar como un camino simple de longitud 0 y al menos dos ciclo. En el caso, donde existan más de dos ciclos, las distancias mínimas entre pares de ciclos cumplen con la condiciones de la prueba anterior, es decir existe al menos dos distancias tal que tienen la misma multiplicidad. Lo cual concluye, que C no es un conjunto profundo de Erdős.

Caso 5: G consiste de un camino simple de longitud al menos 1 y más de un ciclo.

Este caso se reduce al previo, puesto que cada vértice del camino cumple las condiciones del camino de longitud 0 del caso anterior. Por tanto, este caso no es posible.

Caso 6: G no tiene ciclos, consiste de un solo camino simple.

considere $G = P_s$, con $s \geq 1$. Sea $v \in C$, tal que $v - m$ no es un vértice del grafo G, dicho de otra manera, v corresponde con el vértice que da inicio al camino en dirección de las agujas del reloj. Ahora, considere el conjunto $b + C$, con $b \in \mathbb{Z}_n$ tal que $b + v = 0$ y defina $G' = (V(G'), E(G'))$, con $V(G) = b + C$ y $E(G') = E(G)$. Note que G' es subgrafo de $C_m = \{V(G), E(G)\}$, donde $V(C_m) = \langle m \rangle$ y $E(C_m) = E(G)$, esto implica que $b + C$ es un subconjunto del subgrupo cíclico generado por el elemento m. Es así que, $b + C = \{im : i = 0, 1, \ldots, k-1\} = AP(m, s, n)$. Llamando $a = -b$, $k = s$ y $g = m$ se tiene que $C = a + AP(g, k, n)$. Ahora, se verificarán las condiciones que debe cumplir cada progresión. Inicialmente, como m es una distancia, entonces $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$.

Ahora, se probará que, $k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. Suponga lo contrario, es decir, para $C = a + AP(g, k, n)$, con C un conjunto profundo de Erdős, se cumple que $k > \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 = \left\lfloor \frac{|g|}{2} \right\rfloor + 1$.

Por otro lado, según el Lema 3.2, como la máxima multiplicidad en $M(\Delta C)$ $m(g, C) = k - 1$ corresponde con

$$m(g, C) = k - 1 > \left\lfloor \frac{n}{2\gcd(n, g)} \right\rfloor.$$

Luego, como C es profundo de Erdős se tiene que $M(\Delta C) = \{1, \ldots, k-1\}$ y según lo anterior $|M(\Delta C)| > \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$. Igualmente, puesto que, C es un subconjunto del subgrupo generado por g entonces, por el Lema 3.4, $|S(\Delta C)| \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$. Puesto que, $m(g, C) = k - 1$, entonces para cada $d \in S(\Delta C) - \{g\}$, $m(d, C) = i$ con $i \in M(\Delta C) - \{k-1\}$ y $m(d_1, C) \neq m(d_2, C)$, para cada $d_1, d_2 \in S(\Delta C)$, tal que $d_1 \neq d_2$. No obstante, como $S(\Delta C) < M(\Delta C)$, entonces existe un $j \in M(\Delta C) - \{k-1\}$ tal que $j \neq m(d, C)$, para todo $d \in S(\Delta C) - \{g\}$, concluyendo así que C no es de Erdős. Lo cual implica una contradicción. Por tanto, el tamaño $k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. Finalizando así, la prueba.

Reciprocamente, se mostrará que cuando $a = 0$, el conjunto correspondiente a cada uno de los items anteriores corresponde con un conjunto profundo de Erdős.

1. Considere el conjunto $C = \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\} \subseteq \mathbb{Z}_{6c}$ con $c \geq 1$. Calculando su multiconjunto de distancias se tiene que;

$$\Delta C = \left\{\delta\left(\frac{2n}{3},0\right),\delta\left(\frac{2n}{3},\frac{n}{3}\right),\delta\left(\frac{2n}{3},\frac{n}{6}\right),\delta\left(\frac{n}{3},0\right),\delta\left(\frac{n}{3},\frac{n}{6}\right),\delta\left(\frac{n}{6},0\right)\right\}$$

$$\Delta C = \left\{\frac{n}{3},\frac{n}{3},\frac{n}{6},\frac{n}{3},\frac{n}{2},\frac{n}{6}\right\}$$

$$\Delta C = \left\{\left(\frac{n}{2}\right)^1,\left(\frac{n}{6}\right)^2,\left(\frac{n}{3}\right)^3\right\}$$

Tal y como se evidencia en el multiconjunto de distancias anterior, el conjunto C corresponde con un conjunto profundo de Erdős en $\mathbb{Z}_6$. Luego, por el Lema 3.1 para todo $a \in \mathbb{Z}_n$, se tiene que el conjunto $a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$ es un conjunto profundo de Erdős.

2. Por otro lado, tome $C = a + AP(g,k,n)$ con con $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ y $k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. Ahora, por el Lema 3.6 se tiene que $C = a + AP(g,k,n)$ corresponde con un conjunto profundo de Erdős y así, finaliza la prueba.

□

3.1. Contando conjuntos profundos de Erdős

El propósito de esta sección será conocer la cantidad de conjuntos profundos de Erdős en $\mathbb{Z}_n$. Es por ello, que para cada $n > 1$, se considera la familia de conjuntos

$$\mathcal{E}(n) = \{C \subseteq \mathbb{Z}_n : C \textit{ es un conjunto profundo de Erdős}\},$$

y se estudiará su cardinal. Es sabido que por el Teorema 3.10, todo conjunto profundo de Erdős en $\mathbb{Z}_n$ es una progresión aritmética $a + AP(g,k,n)$, con $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, $2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$ y $a \in \mathbb{Z}_n$, ó es el conjunto $a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, para $n = 6c$, con $c \geq 1$, y $a \in \mathbb{Z}_n$. Observe que si se define para cada $n > 1$ las familias

- $\mathcal{F}_1(n) = \left\{a + AP(g,k,n) : 1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor \wedge 2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 \wedge a \in \mathbb{Z}_n\right\}$,
- $\mathcal{F}_2(n) = \begin{cases} \left\{a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\} : a \in \mathbb{Z}_n\right\} & \text{si } n = 6c, \\ \varnothing & \text{si } n \neq 6c, \end{cases}$

se puede reescribir $\mathcal{E}(n)$ en términos de $\mathcal{F}_1(n)$ y $\mathcal{F}_2(n)$ de la siguiente manera:

$$\mathcal{E}(n) = \mathcal{F}_1(n) \cup \mathcal{F}_2(n). \tag{17}$$

Dado que para cada $n > 1$ las familias $\mathcal{F}_1(n)$ y $\mathcal{F}_2(n)$ son disjuntas, estudiar el cardinal de $\mathcal{E}(n)$ se reduce a estudiar el cardinal de $\mathcal{F}_1(n)$ y $\mathcal{F}_2(n)$.

Inicialmente, se analizará la familia de conjuntos $\mathcal{F}_1(n)$, la cual se corresponde con la familia de AP's en $\mathbb{Z}_n$ que son conjuntos profundos de Erdős. Para ello, se consideraran $AP_1 = a_1 + AP(g_1, k_1, n), AP_2 = a_2 + AP(g_2, k_2, n) \in \mathcal{F}_1(n)$, y la relación $\mathcal{R} \subseteq \mathcal{F}_1(n) \times \mathcal{F}_1(n)$, definida como:

$$AP_1 \sim AP_2 \Leftrightarrow g_1 = g_2. \tag{18}$$

Ya establecida $\mathcal{R}$, se tiene el siguiente resultado:

Proposición 3.11. *la relación $\mathcal{R}$ es una relación de equivalencia.*

Demostración. Vamos a mostrar que $\mathcal{R}$ es una relación reflexiva, simétrica y transitiva. Dadas $AP_1 = a_1 + AP(g_1, k_1, n)$, $AP_2 = a_2 + AP(g_2, k_2, n)$ y $AP_3 = a_3 + AP(g_3, k_3, n) \in \mathcal{F}_1(n)$, tenemos:

1. Reflexiva. Para la progresión $AP_1 = a_1 + AP(g_1, k_1, n)$, como $g_1 = g_1$ entonces $AP_1 \sim AP_1$. Por tanto, $\mathcal{R}$ es reflexiva.

2. Simétrica. Suponga que $AP_1 \sim AP_2$ entonces $g_1 = g_2$. Luego, se tiene que $g_2 = g_1$ y en consecuencia $AP_2 \sim AP_1$. Por tanto $\mathcal{R}$ es simétrica.

3. Transitiva. Suponga que $AP_1 \sim AP_2$ y $AP_2 \sim AP_3$. Como consecuencia de la suposición anterior se deduce que; $g_1 = g_2$ y $g_2 = g_3$. Consecuentemente, $g_1 = g_3$ y por lo tanto, $AP_1 \sim AP_3$. Por tanto $\mathcal{R}$ es transitiva.

Por tanto, $\mathcal{R}$ es una relación de equivalencia. □

Ahora, con base en la Proposición 3.11 la clase de equivalencia de la progresión $AP_1 = a_1 + AP(g_1, k, n)$, respecto a la relación $\mathcal{R}$, esta dada por:

$$[AP_1]_{\mathcal{R}} = \{a + AP(g, k, n) : g = g_1\}. \tag{19}$$

De ahí, que $[AP_1]_{\mathcal{R}}$ corresponde al conjunto de todas las progresiones aritméticas tal que su generador es g_1. Esto permite caracterizar cada clase de equivalencia a partir del generador de uno de sus representantes; es decir, la clase de equivalencia de cualquier progresión $a + AP(g, k, n)$ se caracteriza por su generador g. Se denotará la clase de equivalencia de la progresión $a + AP(g, k, n)$ por $[g]_{\mathcal{R}}$, es decir:

$$[a + AP(g, k, n)]_{\mathcal{R}} = [g]_{\mathcal{R}}\,. \tag{20}$$

Dado que las clases de equivalencia forman una partición de $\mathcal{F}_1(n)$ y por el Lema 3.3 cada generador g satisface que $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, entonces

$$\mathcal{F}_1(n) = \bigcup_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} [g]_{\mathcal{R}}\,. \tag{21}$$

Luego, como las clases de equivalencia son disjuntas, por el principio de inclusión exclusión se deduce que

$$|\mathcal{F}_1(n)| = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left|[g]_{\mathcal{R}}\right|\,. \tag{22}$$

De lo anterior, para conocer el cardinal de $\mathcal{F}_1(n)$ es necesario calcular $\left|[g]_{\mathcal{R}}\right|$, para cada $g \in \mathbb{Z}_n$, tal que $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$. Es por ello, que se establece la relación $\mathcal{T}_g \subseteq [g]_{\mathcal{R}} \times [g]_{\mathcal{R}}$, la cual establece, que para $AP_1 = a_1 + AP(g, k_1, n)$ y $AP_2 = a_2 + AP(g, k_2, n) \in [g]_{\mathcal{R}}$

$$AP_1 \sim AP_2 \Leftrightarrow k_1 = k_2. \tag{23}$$

Note que, así como la relación $\mathcal{R}$, la relación $\mathcal{T}_g$ también corresponde con una relación de equiva-

lencia.

Proposición 3.12. *Para todo $g \in \mathbb{Z}_n$, con $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, la relación $\mathcal{T}_g$ corresponde con una relación de equivalencia.*

Demostración. Sean $AP_1 = a_1 + AP(g, k_1, n)$, $AP_2 = a_2 + AP(g, k_2, n)$ y $AP_3 = a_3 + AP(g, k_3, n) \in [g]_{\mathcal{R}}$. Luego, se verifican las siguientes las condiciones:

1. Reflexiva. Para la progresión $AP_1 = a_1 + AP(g, k_1, n)$, como $k_1 = k_1$ entonces $AP_1 \sim AP_1$. Por tanto, $\mathcal{T}_g$ es reflexiva.

2. Simétrica. Suponga que $AP_1 \sim AP_2$ entonces $k_1 = k_2$. Luego, por la simetría de las igualdades se tiene que $k_2 = k_1$ y en consecuencia $AP_2 \sim AP_1$. Por tanto $\mathcal{T}_g$ es simétrica.

3. Transitiva. Suponga que $AP_1 \sim AP_2$ y $AP_2 \sim AP_3$. Como consecuencia de la suposición anterior se deduce que; $k_1 = k_2$ y $k_2 = k_3$. Consecuentemente, $k_1 = k_3$ y por lo tanto, $AP_1 \sim AP_3$. Puesto que para todo $\mathcal{T}_g$ es transitiva.

Por tanto, $\mathcal{T}_g$ corresponde con una relación de equivalencia. □

Por consiguiente, con base en la Proposición 3.12 la clase de equivalencia de la progresión $AP_1 = a_1 + AP(g, k_1, n)$, respecto a la relación $\mathcal{T}_g$, se definen como:

$$[AP_1]_{\mathcal{T}_g} = \{a + AP(g, k, n) : k = k_1\}. \tag{24}$$

Es así, que la clase de equivalencia $[AP_1]_{\mathcal{T}_g}$ corresponde con el conjunto de todas las progresiones aritméticas, tal que sus tamaños son el mismo. Es por ello, que la clase de equivalencia de cualquier progresión $a + AP(g, k, n) \in [g]_{\mathcal{R}}$ de tamaño k, se le distinguirá como

$$[a + AP(g, k, n)]_{\mathcal{T}_g} = [k]_{\mathcal{T}_g}. \tag{25}$$

Puesto que, el tamaño k depende directamente del generador g, pues $2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$, se tiene que

$$[g]_{\mathcal{R}} = \bigcup_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} [k]_{\mathcal{T}_g}. \tag{26}$$

Luego, como las clases de equivalencias son disjuntas dos a dos, entonces

$$\left|[g]_{\mathcal{R}}\right| = \sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_g}\right|. \tag{27}$$

Es así, que con base en la ecuación (22) se deduce que

$$|\mathcal{F}_1(n)| = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_g}\right| \right). \tag{28}$$

Ahora, para encontrar una fórmula explicita para $|\mathcal{F}_1(n)|$, basta con encontrar el valor, $\left|[k]_{\mathcal{T}_g}\right|$. Ya que, $[k]_{\mathcal{T}_g}$ corresponde al conjunto de todas las progresiones aritméticas con un mismo generador $g \in \mathbb{Z}_n$ y tamaño $k \in \mathbb{N}$, entonces $[k]_{\mathcal{T}_g}$ es el conjunto de todas las traslaciones de la $AP(g, k, n)$. Luego, por el Teorema 3.5 si $AP(g, k, n) \neq \left\{0, \frac{n}{2}\right\}$, entonces $\left|[k]_{\mathcal{T}_g}\right| = n$, caso contrario $\left|[k]_{\mathcal{T}_g}\right| = \frac{n}{2}$. Por consiguiente, el siguiente resultado recopila la construcción anterior y establece el primer resultado sobre la cantidad de conjuntos profundos en $\mathbb{Z}_n$.

Lema 3.13. *Para todo $n > 1$*

$$|\mathcal{F}_1(n)| = f_1(n) + n \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\lfloor \frac{n}{2\gcd(n, g)} \right\rfloor, \tag{29}$$

donde $f_1 : \mathbb{N} \setminus \{1\} \to \mathbb{Z}$ está dada por

$$f_1(n) = \begin{cases} -\frac{n}{2} & \textit{si } n \textit{ es par,} \\ 0 & \textit{si } n \textit{ es impar.} \end{cases}$$

Demostración. Para está prueba se consideran dos casos:

Caso 1: Si n es par. Suponga que $g = \frac{n}{2}$, entonces $AP(g, k, n) = \left\{0, \frac{n}{2}\right\}$, lo cual implica que

$\left|[k]_{\mathcal{T}_g}\right| = \frac{n}{2}$. Caso contrario; es decir, cuando $g \neq \frac{n}{2}$, tenemos $\left|[k]_{\mathcal{T}_g}\right| = n$. Con base en lo anterior y en la ecuación (28), se deduce que

$$\begin{aligned}
|\mathcal{F}_1(n)| &= \sum_{g=1}^{\frac{n}{2}} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_g}\right| \right) = \sum_{g=1}^{\frac{n}{2}-1} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_{\frac{n}{2}}}\right| \right) + \sum_{k=2}^{\left\lfloor \frac{n}{2\gcd\left(n,\frac{n}{2}\right)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_{\frac{n}{2}}}\right| \\
&= \sum_{g=1}^{\frac{n}{2}-1} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} n \right) + \sum_{k=2}^{2} \frac{n}{2} = n \sum_{g=1}^{\frac{n}{2}-1} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \right) + \frac{n}{2} \\
&= n \sum_{g=1}^{\frac{n}{2}-1} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + n - \frac{n}{2} = n \left(\sum_{g=1}^{\frac{n}{2}-1} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 \right) - \frac{n}{2} \\
&= n \left(\sum_{g=1}^{\frac{n}{2}-1} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + \left\lfloor \frac{n}{2\gcd\left(n,\frac{n}{2}\right)} \right\rfloor \right) - \frac{n}{2} = n \sum_{g=1}^{\frac{n}{2}-1} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor - \frac{n}{2}.
\end{aligned}$$

Caso 2: Si n impar. En este caso $g \neq \frac{n}{2}$. Por tanto, $\left|[k]_{\mathcal{T}_g}\right| = n$. Luego, con base en la ecuación (28), se deduce que

$$|\mathcal{F}_1(n)| = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} \left|[k]_{\mathcal{T}_g}\right| \right) = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left(\sum_{k=2}^{\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1} n \right) = n \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor.$$

Finalmente, considerando la función $f_1 : \mathbb{N} \setminus \{1\} \to \mathbb{Z}$ dada por:

$$f_1(n) = \begin{cases} -\frac{n}{2} & \textit{si } n \textit{ es par}, \\ 0 & \textit{si } n \textit{ es impar}. \end{cases}$$

se concluye que

$$|\mathcal{F}_1(n)| = f_1(n) + n \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor.$$

□

Con lo anterior previamente establecido, el siguiente paso de este estudio será calcular el cardinal de la familia de conjuntos $\mathcal{F}_2(n)$. Puesto que $\mathcal{F}_2(n) = \left\{ a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\} : a \in \mathbb{Z}_n \right\}$ ó $\mathcal{F}_2(n) = \varnothing$, se con-

centraran los esfuerzos en encontrar el cardinal del primer caso. Dado que si $n = 6c$, con $c \in \mathbb{N}$, $\mathcal{F}_2(n)$ consiste en traslaciones del conjunto $\left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, es suficiente determinar cuantas de estas traslaciones hay.

Lema 3.14. *Todo conjunto de la forma $C = \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, con $n = 6c, c \geq 1$ y $a \in \mathbb{Z}_n$, tiene n traslaciones distintas.*

Demostración. Para mostrar lo anterior basta con corroborar que para todo $a_1, a_2 \in \mathbb{Z}_n$, con $a_1 \neq a_2$, se tiene que $a_1 + C \neq a_2 + C$. Note que el conjunto $C = \left\langle \frac{n}{3} \right\rangle \cup \left\{\frac{n}{6}\right\}$. Además, para cualquier $a \in \mathbb{Z}_n$, $a + C = a + \left\langle \frac{n}{3} \right\rangle \cup a + \left\{\frac{n}{6}\right\}$. Sea $a_1, a_2 \in \mathbb{Z}_n$. Observe que si $a_1 \neq a_2$, entonces $a_1 + \frac{n}{6} \neq a_2 + \frac{n}{6}$. Lo anterior implica que $a_1 + \left\{\frac{n}{6}\right\} \neq a_2 + \left\{\frac{n}{6}\right\}$. Por otro lado, si $a_1 \neq a_2$ no necesariamente se tiene que $a_1 + \left\langle \frac{n}{3} \right\rangle \neq a_2 + \left\langle \frac{n}{3} \right\rangle$. Por esta razón, se supondrán dos casos.

Caso 1: $a_1 + \left\langle \frac{n}{3} \right\rangle = a_2 + \left\langle \frac{n}{3} \right\rangle$. Note que, como $a_1 + \left\{\frac{n}{6}\right\} \neq a + {}_2\left\{\frac{n}{6}\right\}$, entonces $\left(a_1 + \left\langle \frac{n}{3} \right\rangle\right) \cup \left(a_1 + \left\{\frac{n}{6}\right\}\right) \neq \left(a_2 + \left\langle \frac{n}{3} \right\rangle\right) \cup \left(a_2 + \left\{\frac{n}{6}\right\}\right)$ y por tanto $a_1 + C \neq a_2 + C$.

Caso 2: $a_1 + \left\langle \frac{n}{3} \right\rangle \neq a_2 + \left\langle \frac{n}{3} \right\rangle$. Para este caso, como $\left\langle \frac{n}{3} \right\rangle$ es un subgrupo de $\mathbb{Z}_n$, entonces las clases laterales $a_1 + \left\langle \frac{n}{3} \right\rangle$ y $a_2 + \left\langle \frac{n}{3} \right\rangle$ son disjuntas, es decir $\left(a_1 + \left\langle \frac{n}{3} \right\rangle\right) \cap \left(a_2 + \left\langle \frac{n}{3} \right\rangle\right) = \varnothing$. Puesto que, $\left|a_1 + \left\langle \frac{n}{3} \right\rangle\right| = \left|a_2 + \left\langle \frac{n}{3} \right\rangle\right| = 3$, entonces los conjuntos $a_1 + \left\langle \frac{n}{3} \right\rangle$ y $a_2 + \left\langle \frac{n}{3} \right\rangle$ difieren en tres elementos. Por tanto, $\left(a_1 + \left\langle \frac{n}{3} \right\rangle\right) \cup \left(a_1 + \left\{\frac{n}{6}\right\}\right) \neq \left(a_2 + \left\langle \frac{n}{3} \right\rangle\right) \cup \left(a_2 + \left\{\frac{n}{6}\right\}\right)$ y en consecuencia, $a_1 + C \neq a_2 + C$. Es así que, el conjunto C tiene n traslaciones en $\mathbb{Z}_n$. □

En consecuencia del lema anterior, cuando $n = 6c$, con $c \geq 1$, existen n conjuntos profundos de Erdős de la forma $a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, para todo $a \in \mathbb{Z}_n$. Por tanto, se tiene el siguiente resultado.

Lema 3.15. *Para todo $n > 1$,*

$$|\mathcal{F}_2(n)| = \begin{cases} n & si\ n = 6c, \\ 0 & si\ n \neq 6c. \end{cases}$$

Demostración. Si $n \neq 6c$, con $c \geq 1$. entonces $\mathcal{F}_2(n) = \varnothing$, por tanto $|\mathcal{F}_2| = 0$. Caso contrario, si $n = 6c$, con $c \geq 1$, entonces $\mathcal{F}_2(n) = \left\{a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\} : a \in \mathbb{Z}_n\right\}$. Luego, por el Lema 3.14, el conjunto $\left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$ tiene n traslaciones, por lo tanto $|\mathcal{F}_2(n)| = n$. □

Con base en los resultados previos, se establece el primer resultado que nos permite determinar cuantos conjuntos profundos de Erdős hay en $\mathbb{Z}_n$.

Teorema 3.16. *Para todo $n > 1$, la cantidad de conjuntos profundos de Erdős en $\mathbb{Z}_n$ es:*

$$|\mathcal{E}(n)| = f_2(n) + n \sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor$$

Donde, $f_2 : \mathbb{N} \setminus \{1\} \to \mathbb{Z}$ es la función dada por:

$$f_2(n) = \begin{cases} \frac{n}{2} & \textit{si, } n \textit{ es par y es múltiplo de 3,} \\ 0 & \textit{si, } n \textit{ es impar,} \\ -\frac{n}{2} & \textit{si, } n \textit{ es par y no es múltiplo de 3.} \end{cases}$$

Demostración. Dado que $\mathcal{E}(n) = \mathcal{F}_1(n) \cup \mathcal{F}_2(n)$ y $\mathcal{F}_1(n) \cap \mathcal{F}_2(n) = \varnothing$, entonces por el principio de inclusión exclusión se tiene que

$$|\mathcal{E}(n)| = |\mathcal{F}_1(n)| + |\mathcal{F}_2(n)| . \tag{30}$$

Luego, por los Lemas 3.13 y 3.15, se deduce que

$$|\mathcal{E}(n)| = f_1(n) + n \sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + |\mathcal{F}_2(n)| . \tag{31}$$

Finalmente, se mostrará que tomando $f_2(n) = f_1(n) + |\mathcal{F}_2(n)|$ se tiene el resultado. Si n es par, consideramos dos casos: si n múltiplo de 3, entonces n múltiplo de 6, de ahí que $f_1(n) = -\frac{n}{2}$ y $|\mathcal{F}_2(n)| = n$, por lo tanto, $f_2(n) = -\frac{n}{2} + n = \frac{n}{2}$. Además, si n no es múltiplo de 3, entonces n que no es múltiplo de 6, así que $f_1(n) = -\frac{n}{2}$ y $|\mathcal{F}_2(n)| = 0$, por lo tanto $f_2(n) = -\frac{n}{2} + 0 = -\frac{n}{2}$. Si n es impar, entonces $f_1(n) = |\mathcal{F}_2(n)| = 0$, lo cual implica que $f_2(n) = 0$. □

Ejemplo 3.4. Sea $n = 5$, según el Teorema 3.16, la cantidad de conjuntos profundos de Erdős en $\mathbb{Z}_n$ está

dada por,

$$\begin{aligned}|\mathcal{E}(5)| &= f_2(5) + 5\sum_{g=1}^{\lfloor\frac{5}{2}\rfloor}\left\lfloor\frac{5}{2\gcd(5,g)}\right\rfloor,\\ &= 0 + 5\sum_{g=1}^{2}\left\lfloor\frac{5}{2\gcd(5,g)}\right\rfloor,\\ &= 5\left(\left\lfloor\frac{5}{2}\right\rfloor + \left\lfloor\frac{5}{2}\right\rfloor\right) = 5(2+2) = 20.\end{aligned}$$

Por tanto, hay 20 conjuntos profundos de Erdős, los cuales son,

$\{0,1\}$; $\{0,2\}$; $\{0,3\}$; $\{0,4\}$; $\{1,2\}$; $\{1,3\}$; $\{1,4\}$; $\{2,3\}$; $\{2,4\}$; $\{3,4\}$; $\{0,1,2\}$; $\{0,1,3\}$; $\{0,1,4\}$; $\{0,2,3\}$; $\{0,2,4\}$; $\{0,3,4\}$; $\{1,2,3\}$; $\{1,2,4\}$; $\{1,3,4\}$; $\{2,3,4\}$.

En el caso particular de contar cuantos conjuntos de Erdős hay en $\mathbb{Z}_p$, con p se tiene el resultado siguiente.

Corolario 3.17. *Sea $p > 2$ un número primo. Entonces*

$$|\mathcal{E}(p)| = p\left(\frac{p-1}{2}\right)^2.$$

Demostración. Por el Teorema 3.16 se tiene que:

$$|\mathcal{E}(p)| = f_2(p) + p\sum_{g=1}^{\lfloor\frac{p}{2}\rfloor}\left\lfloor\frac{p}{2\gcd(p,g)}\right\rfloor = p\sum_{g=1}^{\lfloor\frac{p}{2}\rfloor}\left\lfloor\frac{p}{2\gcd(p,g)}\right\rfloor.$$

Dado que $\left\lfloor\frac{p}{2}\right\rfloor = \frac{p-1}{2}$ y $1 \le g \le \frac{p-1}{2}$, entonces $\gcd(g,p) = 1$. Por lo tanto:

$$|\mathcal{E}(p)| = p\sum_{g=1}^{\frac{p-1}{2}}\frac{p-1}{2} = p\left(\frac{p-1}{2}\right)\sum_{g=1}^{\frac{p-1}{2}}1 = p\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right) = p\left(\frac{p-1}{2}\right)^2.$$

□

Los resultados a continuación permiten estudiar la cantidad de conjuntos de profundos de Erdős

en $\mathbb{Z}_n$, con determinado tamaño t. Realizando un análisis similar al usado para contar la cantidad $\mathcal{E}(n)$ de profundos de Erdős en $\mathbb{Z}_n$, se considera el conjunto

$$\hat{\mathcal{E}}(n,t) = \{C \subseteq \mathbb{Z}_n : C \textit{ es un conjunto profundo de Erdős de tamaño } t\}. \tag{32}$$

Con base en el Teorema 3.10, todo conjunto profundo de Erdős es una progresión aritmética modular o un conjunto de la forma $a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, en el caso en que $n = 6t$, con $t \geq 1$. Si C es una progresión aritmética, es decir, $C = a + AP(g,k,n)$, entonces el tamaño de C depende directamente del generador g. Puesto que el tamaño k satisface que $2 \leq k \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$, entonces si $\gcd(n,g) = 1$ tenemos que $2 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$. Por tal motivo, el máximo tamaño que una progresión aritmética puede alcanzar es $\left\lfloor \frac{n}{2} \right\rfloor + 1$. Es así, que todos los posibles tamaños t cumplen que $2 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$. Además, si $C = a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, entonces $|C| = 4$.

Por otro lado, considere los siguientes conjuntos en función de t y n.

- $\hat{\mathcal{F}}_1(n,t) = \left\{a + AP(g,k,n) : 1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor \wedge k = t \wedge a \in \mathbb{Z}_n\right\}$.
- $\hat{\mathcal{F}}_2(n,t) = \begin{cases} \left\{a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}\right\} & si\ n = 6c\ y\ t = 4, \\ \varnothing & si\ n \neq 6c\ o\ t \neq 4. \end{cases}$

De la misma forma que en el caso anterior, $\hat{\mathcal{E}}(n,t) = \hat{\mathcal{F}}_1(n,t) \cup \hat{\mathcal{F}}_2(n,t)$. Ya que $\hat{\mathcal{F}}_1(n,t) \cap \hat{\mathcal{F}}_2(n,t) = \varnothing$, por principio de inclusión exclusión, entonces $|\hat{\mathcal{E}}(n,t)| = |\hat{\mathcal{F}}_1(n,t)| + |\hat{\mathcal{F}}_2(n,t)|$. Por ello, para conocer $|\hat{\mathcal{E}}(n,t)|$ es necesario y suficiente, conocer el valor de $|\hat{\mathcal{F}}_1(n,t)|$ y $|\hat{\mathcal{F}}_2(n,t)|$. Inicialmente se enfocarán los esfuerzos en encontrar el cardinal $|\hat{\mathcal{F}}_1(n,t)|$. Para ello, se tomará en consideración la función escalón unitario ó también conocida como la **función de Heaviside**, $\mu : \mathbb{R} \to \{0,1\}$, dada por

$$\mu(x) = \begin{cases} 0 & si,\ x < 0, \\ 1 & si,\ x \geq 0. \end{cases}$$

Lema 3.18. *Para todo $n > 1$, $g \in \mathbb{Z}_n$ con $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, y $t \in \mathbb{Z}$ con $2 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$, se tiene que*

$$|\hat{\mathcal{F}}_1(n,t)| = n \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t \right) + f_3(n,t), \tag{33}$$

donde $f_3 : \mathbb{N} \setminus \{1\} \times \mathbb{N} \setminus \{1\} \to \mathbb{Z}$ se define por

$$f_3(n,t) = \begin{cases} -\frac{n}{2} & \text{si } n \text{ es par y } t = 2, \\ 0 & \text{si } n \text{ es impar o } t \neq 2. \end{cases}$$

Demostración. Note que para cada $g \in \mathbb{Z}_n$, con $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, y cada $k \in \mathbb{N} \setminus \{1\}$, se cumple que

$$AP(g,k,n) \in \hat{\mathcal{F}}_1(n,t) \quad \text{si y solo si} \quad k = t \text{ y } 2 \leq t \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1. \tag{34}$$

En efecto, si $AP(g,k,n) \in \hat{\mathcal{F}}_1(n,t)$, entonces $AP(g,k,n)$ es un conjunto profundo de Erdős con $k = t$ elementos. Luego del Teorema 3.10 se tiene que $2 \leq t \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. Por lo tanto, $k = t$ y $2 \leq t \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$. Recíprocamente, para $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$, si $2 \leq t \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1$ y $k = t$, entonces del Teorema 3.10, la progresión $AP(g,k,n)$ es un conjunto profundo de Erdős de tamaño t, por lo tanto $AP(g,k,n) \in \hat{\mathcal{F}}_1(n,t)$.

Como el objetivo es contar todos los conjuntos profundos de Erdős de tamaño t, y dado que $t \geq 2$, la Afirmación 34 puede reescribirse de la siguiente manera:

$$AP(g,t,n) \in \hat{\mathcal{F}}_1(n,t) \quad \text{si y solo si} \quad t \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1, \tag{35}$$

Además, aplicando la función de Heaviside, $\mu : \mathbb{R} \to \{0,1\}$ tenemos que:

- $\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t \geq 0$ si y solo si $\mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t \right) = 1$.
- $\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t < 0$ si y solo si $\mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t \right) = 0$.

Con el objetivo en mente, consideremos el conjunto

$$S = \left\{ g \in \mathbb{Z}_n : 1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor \ y\ AP(g,k,n) \in \hat{\mathcal{F}}_1(n,t) \right\}. \tag{36}$$

Note que la función $\hat{\mu} : \left\{1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\} \to \mathcal{P}\left(\left\{1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}\right)$ dada por:

$$\hat{\mu}(g) = \begin{cases} \varnothing & \text{si } \ \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right) = 0, \\ \{g\} & \text{si } \ \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right) = 1, \end{cases}$$

permite reescribir el conjunto S en la forma,

$$S = \bigcup_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \hat{\mu}(g).$$

Además, dado que para cada $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ se cumple que:

- $|\hat{\mu}(g)| = |\{g\}| = 1 = \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right)$,
- $|\hat{\mu}(g)| = |\varnothing| = 0 = \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right)$,

y como S es unión de conjuntos disjuntos entonces

$$|S| = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} |\hat{\mu}(g)| = \sum_{g=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right).$$

Ahora, defina la función $f : \hat{\mathcal{F}}_1(n,t) \to (\mathbb{Z}_n \times S) \setminus H(n,t)$ por:

$$f(a + AP(g,k,n)) = (a,g),$$

donde $h : \mathbb{N} \setminus \{1\} \times \mathbb{N} \setminus \{1\} \to \mathbb{Z}_n \times \left\{\frac{n}{2}\right\}$

$$H(n,t) = \begin{cases} \left\{\left(b, \frac{n}{2}\right) : b \in \left\{\frac{n}{2}, \ldots, n-1\right\}\right\} & \textit{si } n \textit{ es par y } t = 2, \\ \varnothing & \textit{si } n \textit{ es impar o } t = 2. \end{cases}$$

Note que f está bien definida. Puesto que en el caso donde n sea par y $t = 2$, entonces la progresión $AP\left(\frac{n}{2}, 2, n\right) \in \hat{\mathcal{F}}_1(n,t)$. La cual, según el Lema 3.5, posee $\frac{n}{2}$ traslaciones diferentes, es decir que existen dos índices de traslación $a_1, a_2 \in \mathbb{Z}_n$, con $a_1 \neq a_2$ tal que $a_2 + AP\left(\frac{n}{2}, 2, n\right) = a_1 + AP\left(\frac{n}{2}, 2, n\right)$. Es por ello que se definió el codominio de la función f como $(\mathbb{Z}_n \times S) \setminus H(n,t)$. Caso contrario, no se presenta problema alguno.

Además, también se tiene que f es biyectiva. Ya que f **es inyectiva:** Sean $a_1 + AP(g_1, t, n)$ y $a_2 + AP(g_2, t, n) \in \hat{\mathcal{F}}_1(n,t)$ y suponga que $f(a_1 + AP(g_1, t, n)) = f(a_2 + AP(g_2, t, n))$. Por lo anterior, $(a_1, g_1) = (a_2, g_2)$, entonces $a_1 = a_2$ y $g_1 = g_2$. Es así, que $a_1 + AP(g_1, t, n) = a_2 + AP(g_2, t, n)$. Por tanto, f es inyectiva.

f **es sobreyectiva:** Sea $(a, g) \in (\mathbb{Z}_n \times S) \setminus H(n,t)$. Como $g \in S$, entonces existe un progresión de tamaño t; $AP(g, t, n) \in \hat{\mathcal{F}}_1(n,t)$. Luego, considere la progresión $a + AP(g, t, n) \in \hat{\mathcal{F}}_1(n,t)$. Así, $f(a + AP(g, t, n)) = (a, g)$.

Luego, como f es una función biyectiva

$$|\hat{\mathcal{F}}_1(n,t)| = |(\mathbb{Z}_n \times S) \setminus H(n,t)|.$$

Luego, puesto que $H(n,t) \subseteq \mathbb{Z}_n \times S$, entonces $|(\mathbb{Z}_n \times S) \setminus H(n,t)| = |\mathbb{Z}_n \times S| - |H(n,t)|$. Por lo tanto,

$$\begin{aligned} |\hat{\mathcal{F}}_1(n,t)| &= |\mathbb{Z}_n||S| - |H(n,t)|, \\ &= n|S| - |H(n,t)|. \end{aligned}$$

Como $H(n,t)$ es una función a trozos, entonces para el caso donde n es par y $t = 2$, se tiene que $H(n,t) = \left\{\left(b, \frac{n}{2}\right) : b \in \left\{\frac{n}{2}, \ldots, n-1\right\}\right\}$, por tanto $|H(n,t)| = \frac{n}{2}$. Por otro lado, para el caso donde, n es impar ó $t \neq 2$, entonces $|H(n,t)| = 0$. Luego, definiendo la función

$$f_3(n,t) = \begin{cases} -\frac{n}{2} & \textit{si } n \textit{ es par y } t = 2, \\ 0 & \textit{si } n \textit{ es impar o } t \neq 2. \end{cases}$$

Se cumple que, $|H(n,t)| = -f_3(n,t)$. Finalmente, se concluye que

$$|\hat{\mathcal{F}}_1(n,t)| = n|S| - (-f_3(n,t)),$$
$$|\hat{\mathcal{F}}_1(n,t)| = f_3(n,t) + n\sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right).$$

□

Por consiguiente, para el caso $|\hat{\mathcal{F}}_2(n,t)|$ se tiene el siguiente resultado.

Lema 3.19. *Para todo $n > 1$, $g \in \mathbb{Z}_n$ tal que $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ y $2 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$. Se tiene que*

$$|\hat{\mathcal{F}}_2(n,t)| = \begin{cases} n & si\ n = 6c\ y\ t = 4, \\ 0 & si\ n \neq 6c\ o\ t \neq 4. \end{cases}$$

Demostración. Si $n \neq 6c$ ó $t \neq 4$, entonces $\hat{\mathcal{F}}_2(n,t) = \varnothing$, por tanto $|\hat{\mathcal{F}}_2(n,t)| = 0$. Caso contrario, si $n = 6c$ con $c \geq 1$ y $t = 4$, entonces el conjunto $\hat{\mathcal{F}}_2(n,t) = \left\{a + \left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}\right\}$ para $a \in \mathbb{Z}_n$. Luego, por el Lema 3.14, entonces $\left\{0, \frac{2n}{3}, \frac{n}{3}, \frac{n}{6}\right\}$, tiene n traslaciones, por tanto $|\hat{\mathcal{F}}_2(n,t)| = n$. □

Ya establecido los resultados anteriores y como $|\hat{\mathcal{E}}(n,t)| = |\hat{\mathcal{F}}_1(n,t)| + |\hat{\mathcal{F}}_2(n,t)|$, entonces se deduce el siguiente resultado de conteo.

Teorema 3.20. *Para todo $n > 1$, $g \in \mathbb{Z}_n$ tal que $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ y $2 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$*

$$|\hat{\mathcal{E}}(n,t)| = f_4(n,t) + n\sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right)$$

donde $f_4 : \mathbb{N} \setminus \{1\} \times \mathbb{N} \setminus \{1\} \to \mathbb{Z}$

$$f_4(n,t) = \begin{cases} n & si\ n = 6c\ y\ t = 4, \\ 0 & si\ n\ es\ impar\ ó\ t \neq 4\ ó\ t \neq 2, \\ -\frac{n}{2} & si\ n\ es\ par\ y\ t = 2. \end{cases}$$

Demostración. Partiendo del hecho de que

$$|\hat{\mathcal{E}}(n,t)| = |\hat{\mathcal{F}}_1(n,t)| + |\hat{\mathcal{F}}_2(n,t)|$$

Luego, por el Lema 3.18 y 3.19 se deduce que

$$\begin{aligned} |\hat{\mathcal{E}}(n,t)| &= |\hat{\mathcal{F}}_1(n,t)| + |\hat{\mathcal{F}}_2(n,t)|, \\ &= f_3(n,t) + |\hat{\mathcal{F}}_2(n,t)| + n\sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right). \end{aligned}$$

Finalmente, se mostrará que $f_4(n,t) = f_3(n,t) + \left|\hat{\mathcal{F}}_2(n,t)\right|$. Ya que, f_4 y $\hat{\mathcal{F}}_2(n,t)$, están definidas para todo $(n,t) \in \mathbb{N} \setminus \{1\} \times \mathbb{N} \setminus \{1\}$, entonces $\hat{\mathcal{F}}_1(n,t) + \left|\hat{\mathcal{F}}_2(n,t)\right|$, está bien definido.

Si $n = 6c$ con $c \geq 1$ y $t = 4$, se tiene que $f_3(n,t) = 0$ y $|\hat{\mathcal{F}}_2(n,t)| = n$, entonces $f_3(n,t) + |\hat{\mathcal{F}}_2(n,t)| = n = f_4(n,t)$. Si n es par y $t = 2$, entonces $f_3(n,t) = -\frac{n}{2}$ y $|\hat{\mathcal{F}}_2(n,t)| = 0$, por tanto $f_3(n,t) + |\hat{\mathcal{F}}_2(n,t)| = -\frac{n}{2} = f_4(n,t)$. Finalmente, si n es impar ó $t \neq 2$ ó $t \neq 4$, se tiene que $f_3(n,t) = 0$ y $|\hat{\mathcal{F}}_2(n,t)| = 0$ y por tanto, $f_4(n,t) = 0$. Por lo tanto, se concluye que

$$|\hat{\mathcal{E}}(n,t)| = f_4(n,t) + n\sum_{g=1}^{\lfloor \frac{n}{2} \rfloor} \mu\left(\left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1 - t\right).$$

□

Ejemplo 3.5. Utilizando el Teorema 3.19 la cantidad de conjuntos profundos de Erdős en $\mathbb{Z}_{10}$ de tamaño $t = 5$ está dada por,

$$
\begin{aligned}
|\hat{\mathcal{E}}(10,5)| &= f_4(10,5) + 10\sum_{g=1}^{\lfloor \frac{10}{2} \rfloor} \mu\left(\left\lfloor \frac{10}{2\gcd(10,g)} \right\rfloor + 1 - 5\right), \\
&= 0 + 10\sum_{g=1}^{\lfloor 5 \rfloor} \mu\left(\left\lfloor \frac{10}{2\gcd(10,g)} \right\rfloor - 4\right), \\
&= 10\left[\mu\left(\left\lfloor \frac{10}{2\,\gcd(10,1)} \right\rfloor - 4\right) + \mu\left(\left\lfloor \frac{10}{2\,\gcd(10,2)} \right\rfloor - 4\right),\right. \\
&\quad + \mu\left(\left\lfloor \frac{10}{2\,\gcd(10,3)} \right\rfloor - 4\right) + \mu\left(\left\lfloor \frac{10}{2\,\gcd(10,4)} \right\rfloor - 4\right) \\
&\quad \left. + \mu\left(\left\lfloor \frac{10}{2\,\gcd(10,5)} \right\rfloor - 4\right)\right] \\
&= 10\left[\mu(1) + \mu(-2) + \mu(1) + \mu(-2) + \mu(-3)\right], \\
&= 10(1 + 0 + 1 + 0 + 0) = 20.
\end{aligned}
$$

De ahí, hay veinte conjuntos profundos de Erdős en $\mathbb{Z}_{10}$ de tamaño cinco. Los cuales, se muestran a continuación,

$$\{0,1,2,3,4\}\,;\{0,1,2,3,9\}\,;\{0,1,2,8,9\}\,;\{0,1,3,4,7\}\,;\{0,1,4,7,8\}\,;$$

$$\{0,1,7,8,9\}\,;\{0,2,3,6,9\}\,;\{0,3,4,6,7\}\,;\{0,3,6,7,9\}\,;\{0,6,7,8,9\}\,;$$

$$\{1,2,3,4,5\}\,;\{1,2,4,5,8\}\,;\{1,2,5,8,9\}\,;\{1,4,5,7,8\}\,;\{2,3,4,5,6\}\,;$$

$$\{2,3,5,6,9\}\,;\{2,5,6,8,9\}\,;\{3,4,5,6,7\}\,;\{4,5,6,7,8\}\,;\{5,6,7,8,9\}\,.$$

Corolario 3.21. *Sea $p > 2$ un número primo, $g \in \mathbb{Z}_n$ tal que $1 \leq g \leq \left\lfloor \frac{n}{2} \right\rfloor$ y $2 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$, entonces*

$$\left|\hat{\mathcal{E}}(p,t)\right| = \binom{p}{2}. \tag{37}$$

Demostración. Con base en el Teorema 3.19 tenemos:

$$|\hat{\mathcal{E}}(p,t)| = f_4(p,t) + p\sum_{g=1}^{\lfloor \frac{p}{2} \rfloor} \mu\left(\left\lfloor \frac{p}{2\gcd(p,g)} \right\rfloor + 1 - t\right).$$

Ya que p es primo impar, entonces $f_4(p,t) = 0$ y $(g,p) = 1$ para todo $g \in \mathbb{Z}_n$. Por tanto,

$$|\hat{\mathcal{E}}(p,t)| = p\sum_{g=1}^{\lfloor \frac{p}{2} \rfloor} \mu\left(\left\lfloor \frac{p}{2\gcd(p,g)} \right\rfloor + 1 - t\right) = p\sum_{g=1}^{\frac{p-1}{2}} \mu\left(\frac{p-1}{2} + 1 - t\right)$$
$$= p\sum_{g=1}^{\frac{p-1}{2}} \mu\left(\frac{p+1}{2} - t\right).$$

Luego, para todo $1 \leq t \leq \left\lfloor \frac{p}{2} \right\rfloor + 1 = \frac{p+1}{2}$. Por tanto, $0 \leq \frac{p+1}{2} - t$, lo cual, implica que $\mu\left(\frac{p+1}{2} - t\right) = 1$ y por lo tanto

$$p\sum_{g=1}^{\frac{p-1}{2}} \mu\left(\frac{p+1}{2} - t\right) = p\sum_{g=1}^{\frac{p-1}{2}} 1 = p\left(\frac{p-1}{2}\right) = \binom{p}{2}.$$

□

4. s-Familias profundas de Erdős

Las primeras nociones sobre el concepto de s-familias profundas de Erdős fueron introducidas por Gaede (2022), el cual en su investigación enfocó sus esfuerzos en estudiar a detalle lo que él denominó **pares de Erdős**, los cuales definió como las familias de 2 progresiones aritméticas modulares, $\{C_1, C_2\}$, y el multiconjunto $\Delta C_1 \uplus \Delta C_2 = \{d^{m(d,C_1)+m(d,C_2)} : d \in S(\Delta C_1) \cup S(\Delta C_2)\}$ corresponde con un multiconjunto de Erdős. En otras palabras, Gaede investigó ¿cuándo la suma ($\uplus$) de dos multiconjuntos de Erdős, de progresiones aritméticas, da otro multiconjunto de Erdős?

El siguiente ejemplo ilustra el concepto de este multiconjuto de Erdős.

Ejemplo 4.1. Sean $C_1 = \{2,5,7\}$ y $C_2 = \{0,2,4\} \subseteq \mathbb{Z}_8$ conjuntos profundos de Erdős. Luego, sabiendo que $\Delta C_1 = \{2^1, 3^2\}$ y $\Delta C_2 = \{4^1, 2^2\}$, se tiene que:

$$\Delta C_1 \uplus \Delta(C_2) = \{d^{m(d,C_1)+m(d,C_2)} : d \in \{2,3,4\}\} = \{2^{1+2}, 3^2, 4^1\} = \{4^1, 3^2, 2^3\}.$$

En consecuencia, el multiconjunto $\Delta C_1 \uplus \Delta C_2$ se corresponde con un multiconjunto de Erdős.

Gaede(2022) estableció como objetivo de investigación encontrar una caracterización detallada para los pares de Erdős. Es así, que para poder analizar estas estructuras, Gaede decide generalizar la teoría de los conjuntos profundos de Erdős extendiendo las definiciones presentadas en el capítulo anterior a las familias conformadas por subconjuntos de $\mathbb{Z}_n$.

En esta sección $\mathcal{F}$ denotará una familia $\{C_1, \ldots, C_s\}$ de subconjuntos de $\mathbb{Z}_n$, con $|C_j| > 1$, para todo $1 \leq j \leq s$.

Definición 4.1 (Multiconjunto de distancias para una familia de subconjuntos)**.** El multiconjunto de distancias de $\mathcal{F}$, denotado por $\Delta\mathcal{F}$, se define como:

$$\Delta\mathcal{F} = \biguplus_{j=1}^{s} \Delta(C_j) = \left\{ d^{\sum_{j=1}^{s} m(d,C_j)} : d \in \bigcup_{j=1}^{s} S(\Delta(C_j)) \right\}. \tag{38}$$

Definición 4.2 (Soporte del multiconjunto de distancias para una familia)**.** El soporte de $\Delta\mathcal{F}$, denotado por $S(\Delta\mathcal{F})$, se define como

$$S(\Delta\mathcal{F}) = \bigcup_{j=1}^{s} S(\Delta(C_j)), \tag{39}$$

donde $S(\Delta(C_j))$, con $1 \leq j \leq s$, es el soporte de lo multiconjuntos de distancias de cada subconjunto de $\mathbb{Z}_n$ que conforma la familia $\mathcal{F}$.

Definición 4.3 (Multiplicidades de las distancias para una familia)**.** Sea $d \in S(\Delta\mathcal{F})$. La multiplicidad del elemento d, denotada por $m(d, \mathcal{F})$, se define como:

$$m(d, \mathcal{F}) = \sum_{j=1}^{s} m(d, C_j) = \sum_{j=1}^{s} |\{\{x, y\} \subseteq C_j : x \neq y \wedge \delta(x, y) = d\}|. \tag{40}$$

Definición 4.4. (Conjunto de multiplicidades para una familia de subconjuntos) El conjunto de multiplicidades de $\Delta\mathcal{F}$ se define como:

$$M(\Delta\mathcal{F}) = \{m(d, \mathcal{F}) : d \in S(\Delta\mathcal{F})\}. \tag{41}$$

Así como en la sección anterior, el concepto fundamental es el de conjunto profundo de Erdős, en

esta sección el concepto principal corresponde con el de la siguiente definición:

Definición 4.5 (s-Familias profundas de Erdős)**.** Sea $\mathcal{F} = \{C_1, \ldots, C_s\}$ una familia de subconjuntos no vacíos de $\mathbb{Z}_n$. Se dice que $\mathcal{F}$ es una s-familia de Erdős, si $C_1, \ldots, C_s$ son conjuntos profundos de Erdős y existe un $k \in \mathbb{N}$ tal que, para cada $i \in \{1, \ldots, k-1\}$ existe una distancia d_i que satisface:

$$m(d_i, \mathcal{F}) = \sum_{j=1}^{s} |\{\{x, y\} \subseteq C_j : \delta(x, y) = d_i\}| = i. \tag{42}$$

Observación 6. Una familia $\mathcal{F} = \{C_1, \ldots, C_r\}$ de subconjuntos no vacíos de $\mathbb{Z}_n$ es una s-familia de Erdős si cumple las siguientes condiciones:

1. Cada $C_1, \ldots, C_r$ es un conjunto profundo en $\mathbb{Z}_n$.

2. La función $F : S(\Delta\mathcal{F}) \to M(\Delta\mathcal{F})$, definida como $F(d) = m(d, \mathcal{F})$, es inyectiva.

3. $M(\Delta\mathcal{F}) = \{1, \ldots, k-1\}$ para algún $k \in \mathbb{N}$.

Con la finalidad de aclarar las definiciones anteriores, considere el siguiente ejemplo de una 2-familia de Erdős.

Ejemplo 4.2. Considere la familia $\mathcal{F} = \{\{0, 1, 2, 3, 4, 5\}, \{0, 3, 6, 9\}\}$, de subconjuntos de $\mathbb{Z}_{13}$. Inicialmente, se calcularan el multiconjunto de distancias, por medio de las tablas de distancias, para los conjuntos $C_1 = \{0, 1, 2, 3, 4, 5\}$ y $C_2 = \{0, 3, 6, 9\}$. Es así, que $\Delta C_1 = \{5^1, 4^2, 3^3, 2^4, 1^5\}$ y $\Delta C_2 = \{4^1, 6^2, 3^3\}$. Luego, el multiconjunto de $\mathcal{F}$ se define como:

$$\Delta\mathcal{F} = \Delta C_1 \uplus \Delta C_2 = \{5^1, 4^2, 3^3, 2^4, 1^5, 4^1, 6^2, 3^3\} = \{5^1, 6^2, 4^3, 2^4, 1^5, 3^6\}$$

Por otro lado, se puede verificar que $\mathcal{F}$ es un multiconjunto de Erdős por medio de la definición

Tabla 4

ΔC_1

y \ x	0	1	2	3	4	5
0	·	1	2	3	4	5
1	·	·	1	2	3	4
2	·	·	·	1	2	3
3	·	·	·	·	1	2
4	·	·	·	·	·	1
5	·	·	·	·	·	·

Tabla 5

ΔC_2

y \ x	0	3	6	9
0	·	3	6	4
3	·	·	3	6
6	·	·	·	3
9	·	·	·	·

calculando las multiplicidades de cada distancia en $S(\Delta\mathcal{F}) = \{1, 2, 3, 4, 5, 6\}$

$$m(5,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 5\}| = |\{\{5,0\}\}| = 1,$$

$$m(6,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 6\}| = |\{\{9,3\},\{6,0\}\}| = 2,$$

$$m(4,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 4\}| = |\{\{4,0\},\{5,1\}\}| + |\{9,0\}| = 3,$$

$$m(2,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 2\}| = |\{\{2,0\},\{3,1\},\{4,2\},\{5,3\}\}| = 4,$$

$$m(1,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 1\}| = |\{\{1,0\},\{2,1\},\{3,2\},\{4,3\},\{5,4\}\}| = 5,$$

$$m(3,\mathcal{F}) = \sum_{j=1}^{2} |\{\{x,y\} \subseteq C_j : \delta(x,y) = 3\}| = |\{\{3,0\},\{4,1\},\{5,2\}\}| + |\{\{3,0\},\{6,3\},\{9,6\}\}| = 6.$$

Por tanto, $\mathcal{F}$ es una familia profunda de Erdős y $\Delta\mathcal{F} = \{5^1, 6^2, 4^3, 2^4, 1^5, 3^6\}$.

4.1. 2-Familias Profundas de Erdős (Caso s=2)

Referente al estudio y clasificación de las 2-familias profundas de Erdős se tiene a la investigación diregida por Gaede (2022), el cual estudió un caso particular de 2-familias profundas de Erdős, este corresponde con la caracterización de las familias compuestas por 2 progresiones aritméticas de Erdős. De allí, se formulo el siguiente resultado sobre su caracterización :

Teorema 4.1. *Sea $C_1, C_2 \subseteq \mathbb{Z}_n$, con $C_1 = AP(g_1, k_1, n)$ y $C_2 = AP(g_2, k_2, n)$ conjuntos profundos de Erdős, tales que $3 \leq k_1 \leq k_2 \leq \left\lfloor \frac{n}{2\gcd(n,g)} \right\rfloor + 1, \gcd(n, g_1, g_2) = 1$, y $g_2 \leq \left\lfloor \frac{n}{2} \right\rfloor$. Luego, $\mathcal{F}$ es un par de Erdős, si y solo si*

a. $k_1 = k_2 = 3$ y $g_2 \in \left\{2g_1, \frac{n-g_1}{2}\right\}$ para todo $n \geq 7$ ó

b. $(n, k_1, k_2) \in \{(13, 6, 4), (19, 7, 6), (31, 11, 9)\}$.

En este capitulo se enfocaran los esfuerzos en estudiar un resultado referente al primer ítem del Teorema 4.1, puesto que la prueba de este se mueve alrededor de los conceptos presentados en el primer capitulo del presente trabajo. Dicho resultado se presenta a continuación.

Teorema 4.2. *Sea $\mathcal{F} = \{A_1, A_2\}$ un par de progresiones aritméticas modulares en $\mathbb{Z}_n$, con $A_1 = \{0, g_1, 2g_1\}, A_2 = \{0, g_2, 2g_2\}$, $1 \leq g_1, g_2 \leq \left\lfloor \frac{n}{2} \right\rfloor$. $\mathcal{F}$ es un par de Erdős de Erdős si y solo si, $g_2 \in \left\{2g_1, \frac{n-g_1}{2}\right\}$, donde $n \geq 7$.*

Demostración. Tome $1 \leq g_1, g_2 \leq \left\lfloor \frac{n}{2} \right\rfloor$ y defina $A_1 = AP(g_1, 3, n)$ y $A_2 = AP(g_2, 3, n)$. Note que $g_1 \neq g_2$, de no ser así, $A_1 = A_2$ y en consecuencia, $\Delta(A_1) = \Delta(A_2)$. Luego, para todo $d \in S(\Delta A_1) \cup S(\Delta A_2)$, $m(d, \mathcal{F}) = m(d, A_1) + m(d, A_2) = 2m(d, A_1)$. Por tanto, no existe alguna distancia con multiplicidad 1, lo cual no es posible. Igualmente, $g_1, g_2 < \frac{n}{2}$, ya que si $g_1 = \frac{n}{2}$, entonces $|g_1| = 2$, por tanto $AP(g_1, k, n)$ tendría a lo sumo 2 elementos, lo cual contradice el hecho de que $k = 3$.

Ahora, tome $A_1 = \{0, g_1, 2g_1\}$ y $A_2 = \{0, g_2, 2g_2\}$. Luego, calculando los multiconjuntos de distancias se tiene que

$$\begin{aligned} \Delta A_1 &= \{\delta(0, g_1), \delta(g_1, 2g_1), \delta(0, 2g_1)\}, \\ &= \{|g_1|_n, |g_1|_n, |2g_1|_n\}, \\ &= \left\{g_1^2, |2g_1|_n^1\right\}. \end{aligned}$$

Igualmente, para A_2, se tiene que $\Delta A_2 = \left\{g_2^2, |g_2|_n^1\right\}$. Es así, que

$$\Delta A_1 \uplus \Delta A_2 = \left\{g_1^2, g_2^2, |2g_2|_n^1, |2g_1|_n^1\right\}.$$

Para que, $\Delta A_1 \uplus \Delta A_2$, sea un multiconjunto de Erdős, deben existir tres distancias diferentes en $S(\Delta\mathcal{F})$, es por ello, que $n \geq 7$, ya que es el mínimo valor que permite más de dos progresiones aritméticas diferentes, con más de tres distancias diferentes. Además, se debe cumplir que para ello, $|S(\Delta A_1) \cap S(\Delta A_2)| = 1$. Como las distancias g_1 y g_2 son distintas, entonces se tiene que $g_1 = |2g_2|_n$ ó $g_2 = |2g_1|_n$.

Suponga que, $g_1 = |2g_2|_n$, por definición de distancia se tiene que $g_1 = 2g_2$ ó $g_1 = n - 2g_2$. Luego, suponiendo que $g_1 < g_2$, entonces $2g_1 < 2g_2$, por tanto $g_1 < 2g_2$. Lo cual implica que $g_1 \neq 2g_2$, por tanto solo es posible, que $g_2 = n - 2g_1$.

Por otro lado, si $g_2 = |2g_1|_n$, entonces $g_2 = 2g_1$ ó $g_2 = n - 2g_1$. Por tanto, para $1 \leq g_1 \leq \left\lfloor \frac{n}{2} \right\rfloor$, $g_2 \in \left\{2g_1, n - 2g_1, \frac{n-g_1}{2}\right\}$. Note que tomando $g_2 = n - 2g_1$, entonces $g_1 = \frac{n-g_2}{2}$. Por otro lado, tomando $g_2 = \frac{n-g_1}{2}$, tenemos que $g_1 = n - 2g_2$, luego este caso es análogo al anterior, es decir se genera la misma familia. Por tanto, solo se consideran $1 \leq g_1 \leq \left\lfloor \frac{n}{2} \right\rfloor$, $g_2 \in \left\{2g_1, \frac{n-g_1}{2}\right\}$.

De forma reciproca, considere los siguientes casos.

1. Tome $g_2 = 2g_1$. luego, $\mathcal{F}_1 = \{\{0, g_1, 2g_1\}, \{0, 2g_1, 4g_1\}\}$. Luego, $\Delta\mathcal{F}_1 = \left\{g_1^2, (2g_1)^3, (4g_1)^1\right\}$. Por tanto, $\mathcal{F}_1$ es un par de Erdős.

2. Tome $g_2 = \frac{n-g_1}{2}$. Luego, $\mathcal{F}_1 = \left\{\{0, g_1, 2g_1\}, \left\{0, \frac{n-g_1}{2}, n - g_1\right\}\right\}$. Luego, $\Delta\mathcal{F}_1 = \left\{g_1^3, \left(\frac{n-g_1}{2}\right)^2, (2g_1)^1\right\}$. Por tanto, $\mathcal{F}_2$ es una 2-Familia de Erdős.

□

Ejemplo 4.3. Tome $n = 11$ y $g_1 = 3$, entonces, $g_2 \in \{6, 5, 4\}$ como todo generador cumple que $1 \leq g \leq \left\lfloor \frac{11}{2} \right\rfloor = 5$ se tiene que $g_2 \in \{4, 5\}$.

- Si $g_1 = 3$ y $g_2 = 4$, entonces, $A_1 = \{0, 3, 6\}$ y $A_2 = \{0, 8, 4\}$, en consecuencia, $\Delta A_1 = \{3^2, 5^1\}$ y $\Delta A_2 = \{4^2, 3^1\}$, por tanto, $\Delta A_1 \uplus \Delta A_2 = \left\{5^1, 4^2, 3^3\right\}$.

- Si $g_1 = 3$ y $g_2 = 5$, entonces, $A_1 = \{0, 3, 6\}$ y $A_2 = \{0, 5, 10\}$, en consecuencia, $\Delta A_1 = \{3^2, 5^1\}$ y $\Delta A_2 = \{5^2, 1^1\}$, por tanto, $\Delta A_1 \uplus \Delta A_2 = \left\{1^1, 3^2, 4^3\right\}$.

Ejemplo 4.4. Tome $n = 11$ y $g_1 = 2$, entonces, $g_2 \in \{4, 7\}$ como todo generador cumple que $1 \leq g \leq \left\lfloor \frac{11}{2} \right\rfloor = 5$ se tiene que $g_2 = 4$. Por tanto, $A_1 = \{0, 2, 4\}$ y $A_2 = \{0, 8, 4\}$, en consecuencia, $\Delta A_1 = \{2^2, 4^1\}$ y $\Delta A_2 = \{4^2, 3^1\}$, por tanto, $\Delta A_1 \uplus \Delta A_2 = \left\{3^1, 2^2, 4^3\right\}$.

Para finalizar con la temática de este trabajo de grado y como forma de motivación para futuros trabajos, se establece una conjetura sobre la caracterización de las 2-familias de profundas de Erdős.

Conjetura 4.3. *Toda* 2*-familia profunda de Erdős es un par de Erdős.*

5. Conclusiones

Las s-Familias profundas de Erdős surgieron como el resultado de trasladar el problema original del plano Erdős a $\mathbb{Z}_n$, este último dotado de características propias de un espacio métrico. Durante la realización de este trabajo, se evidenció el poco estudio y rigor que se encuentra en la literatura alrededor de dicho tema. Es por ello, que uno de los enfoques que se tomaron durante la realización del trabajo, fue el de establecer un respaldo teórico, por medio de definiciones, Lemas, Teoremas y demás resultados, sobre las características y estructura de los conjuntos profundos de Erdős (Caso $s = 1$) y una parte de las 2-Familias profundas de Erdős.

Adicionalmente, con este estudio se observó la necesidad de recurrir a la teoría de números, de conjuntos, de grupos y de grafos, para poder caracterizar y demostrar los resultados propuestos. Se espera que este documento sirva como fundamento para seguir ahondando en las s-Familias profundas de Erdős desde su sentido matemático y explorando sus posibles aplicaciones; así como su relación con la música, introducidas por Gaede (2022) y por Toussaint (2013).

Referencias Bibliográficas

Epp, S. S. (2012). *Matemáticas discretas con aplicaciones*. Cengage Learning.

Erdős, P., Jinghuang, T., Leonard, A., Johnsonbaugh, R., Norton, V., Anderson, E. (1982). Elementary Problems: E2938-E2943. *The American Mathematical Monthly, 89*(4), 273–274.

Gaede, T. (2022). *Erdős-Deep families of arithmetic progressions*. [Master's thesis, University of Victoria].

Santos, M. J. (2024). Códigos de conteo [Repositorio de códigos]. GitHub. `https://github.com/MauricioJafetSantos/C-digos-de-conteo`

Santos, M. J. (2024). Códigos de conteo [Repositorio de códigos]. GitHub. `https://github.com/MauricioJafetSantos/Conteos-por-tama-o`

Syropoulos, A. (2001). Mathematics of Multisets. In C. S. Calude, G. Păun, G. Rozenberg, A. Salomaa (Eds.), *Multiset Processing. WMC 2000* (Vol. 2235, pp. 91–103). Springer.

Toussaint, G. (2013). The geometry of musical rhythm: What makes a "good" rhythm good? *Journal of Mathematics and the Arts, 8*(3), 135–137.